Ustawienia bezpieczeństwa w Exchange Server, SharePoint i Lync

Dokument powstał w ramach współpracy w obszarze bezpieczeństwa teleinformatycznego w postaci programu SCP (Security Cooperation Program)

Spis treści

Wstęp

Platforma Office System to nie tylko Word, Excel, PowerPoint czy Outlook, ale cała platforma, w ramach której użytkownicy mogą skorzystać z produktów serwerowych jak i klienckich. Wśród produktów serwerowych to Microsoft Exchange Server jako serwer poczty, Microsoft SharePoint Server jako serwer pracy grupowej czy Microsoft Lync Server jako narzędzie komunikacyjne.

Problemy związane z bezpieczeństwem to najważniejsze wyzwanie dla każdego, kto korzysta ze współczesnych systemów informatycznych. Zagrożenia mogą pochodzić z tak wielu źródeł, że przeciętny użytkownik nie zabezpieczy się przed nimi samodzielnie i skutecznie. Problemy związane z bezpieczeństwem to najważniejsze wyzwanie dla każdego, kto korzysta ze współczesnych systemów informatycznych.

Wszystkie produkty platformy Office budowane są pod katem zapewnienia wysokiego bezpieczeństwa. Bezpieczeństwo to zapewnione jest zgodnie z inicjatywą Trustworthy Computing (TWC). Microsoft utworzył TWC w związku z problemami dotyczącymi bezpieczeństwa jego produktów. Koncepcja Trustworthy Computing (TWC), czyli optymalnej, bezpiecznej platformy komputerowej, opiera się na czterech filarach: bezpieczeństwie, poufności informacji, niezawodności i wiarygodności przedsiębiorstwa.

Filary te zdefiniowane są następująco:

- Bezpieczeństwo - Systemy muszą mieć zabezpieczenia ułatwiające ochronę przed atakami sieciowymi. Bezpieczeństwo systemu oznacza odporność na ataki sieciowe, a także ochronę poufności informacji oraz integralność i dostępność systemu i danych.
- Poufność informacji - Użytkownicy powinni mieć wpływ na bezpieczeństwo i wykorzystanie dotyczących ich danych oraz na weryfikację zgodności procesów gromadzenia, nadzoru i wykorzystania danych z zasadami rzetelnego przetwarzania informacji.
- Niezawodność - Jest to niezbędna gwarancja dostępności funkcji związanych z systemem i programami. Niezawodność oznacza tutaj eliminację usterek, nieprzerwaną dostępność systemu komputerowego i wydajne funkcjonowanie zgodnie z oczekiwaniami.
- Wiarygodność przedsiębiorstwa - gwarancja firmy Microsoft o bezpieczeństwie swoich produktów.

W celu zabezpieczenia pakietu Office oraz dokumentów należy wziąć pod uwagę:

- Opcji prywatności w Office 2013
- Ustawień walidacji plików Office 2013
- Ustawień widoku chronionego (Protected View) w Office 2013
- Ustawień bezpieczeństwa dodatków AddIn w Office 2013
- Ustawień bezpieczeństwa dodatków ActiveX w Office 2013
- Ustawień bezpieczeństwa makr VBA w Office 2013
- Konfiguracji ustawień zaufanych lokalizacji (Trusted Locations) w Office 2013
- Konfiguracji ustawień zaufanych wydawców (Trusted Publishers) w Office 2013

Szczegółowe informacje dotyczące planowania bezpiecznego wdrożenia Office dostępne jest pod adresem: http://technet.microsoft.com/en-us/library/cc178971.aspx

Jednym z elementów zapewnienia bezpieczeństwa jest wsparcie produktów Office dla podpisu cyfrowego. XAdES to najbardziej popularny format podpisu elektronicznego w Polsce. Występuje on w kilku odmianach: zwykły, ze stemplem czasowym, dodatkowymi informacjami itd. Format ten wspierany jest przez platformę Office. Jednocześnie, zgodnie z wymaganiami prawa polskiego, w tym • Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2013 poz. 262), format XAdES jest formatem przyjętym jako obowiązujący dla realizacji niezaprzeczalnego podpisu elektronicznego.

Office 2013 zapewnia następujące poziomy podpisu cyfrowego XAdES

Poziom podpisu	Opis
XAdES-EPES (Base)	Dodaje informację o certyfikacie do podpisu XML-DSig. Jest to standardowa funkcjonalność Office 2013.
XAdES-T (Timestamp)	Dodaje znacznik czasu do sekcji XML-DSig oraz XAdES-EPES podpisu, dzięki czemu chroni dokument przez wygaśnięciem certyfikatu.
XAdES-C (Complete)	Dodaje referencje do łańcucha certyfikacji oraz informacji o statusie unieważnienia.
XAdES-X (Extended)	Dodaje znacznik czasu do elementu XML-DSig SignatureValue oraz sekcji –T i –C podpisu. Dodatkowy znacznik czasu chroni dodatkowe dane przed odrzuceniem.
XAdES-X-L (Extended Long Term)	Przechowuje aktualny certyfikat oraz informacje o unieważnieniu w dodatkowym podpisie. Pozwala to na walidację certyfikatu nawet jeśli certyfikat serwera nie jest już dostępny.

Wszystkie ustawienia związane z podpisem cyfrowym w dokumentach Office możliwe są do skonfigurowanie dla wszystkich użytkowników za pomocą Group Policy. Poniżej w tabeli znajduje się zestawienie ustawień Group Policy dotyczący podpisu cyfrowego.

Ustawienie Group Policy	Opis
Require OCSP at signature generation time	Polisa ta pozwala na ocenę kiedy Office 2013 wymaga danych do unieważnienia dla wszystkich certyfikatów w łańcuchu, kiedy generowane są podpisy cyfrowe. Wykorzystywany jest do tego celu OCSP (Online Certificate Status Protocol).
Specify minimum	Ustawienie tej polisy pozwala na określenie minimalnego poziomu podpisu XAdES (patrz tabela wyżej), które muszą być użyte w aplikacjach Office 2013

XAdES level for digital signature generation	aby stworzyć podpis cyfrowy XAdES. Jeśli aplikacje Office 2013 nie są w stanie użyć minimalnego poziomu, to aplikacja Office nie stworzy podpisu.
Check the XAdES portions of a digital signature	Polisa pozwala określić kiedy Office 2013 sprawdza fragmenty XAdES podpisu cyfrowego podczas walidacji tego podpisu w dokumencie.
Do not allow expired certificates when validating signatures	Ustawienie tej polisy pozwala na konfigurację kiedy Office 2013 akceptuje przedawnione podpisy cyfrowe podczas sprawdzenia podpisu.
Do not include XAdES reference object in the manifest	Ustawienie to pozwala na określenie kiedy referencja do obiektu XAdES pojawi się w manifeście. Należy ustawić wartość parametru na **Enabled** jeśli chcemy oby Office 2007 mógł otwierać dokumenty Office 2013 z podpisem XAdES. W przeciwnym wypadku Office 2007 określi go jako nieprawidłowy.
Select digital signature hashing algorithm	Polisa ta pozwala na konfigurację algorytmu haszującego, który będzie używany przez aplikacje Office 2013 do potwierdzenia podpisu cyfrowego.
Set signature verification level	Ustawienie to pozwala określić poziom weryfikacji, który będzie używany przez Office 2013 podczas walidacji podpisu cyfrowego.
Requested XAdES level for signature generation	Polisa ta pozwala na określenie żądanego lub oczekiwanego poziomu XAdES w tworzonym podpisie cyfrowym.

Wszystkie te ustawienia Group Policy są umieszczone w rejestrze w kluczu:
\software\policies\microsoft\office\15.0\common\signatures!:

Podpis cyfrowy w Office

Podpis cyfrowy, czyli inaczej podpis elektroniczny. Najkrócej mówiąc są to dane służące identyfikacji osoby składającej podpis elektroniczny oraz do potwierdzania autentyczności dokumentu,

który to zapisany jest w postaci elektronicznej. Zastosowanie takiego podpisu daje nam gwarancję autentyczności danych oraz potwierdza tożsamość osoby wysyłającej dane.

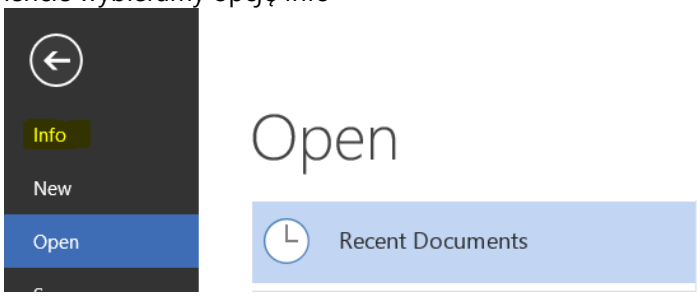
Podpis cyfrowy jest unikatową wartością dołączaną do pliku przez specjalne oprogramowanie. Stworzenie podpisu jest dwuetapowe – w pierwszej kolejności obliczana jest funkcja skrótu (hash) na bazie zawartości pliku. Następnie mając obliczoną funkcję przy pomocy klucza prywatnego szyfrowana jest zawartość. Dzięki posługiwaniu się podpisem elektronicznym przesyłane dokumenty elektroniczne są zabezpieczone przed modyfikacją przez osoby nieupoważnione. Każda, nawet przypadkowa, zmiana w treści przesyłki przez osoby niepowołane powoduje usunięcia podpisu oraz poinformowanie o tym fakcie użytkownika.

Podpis cyfrowy w Microsoft Office

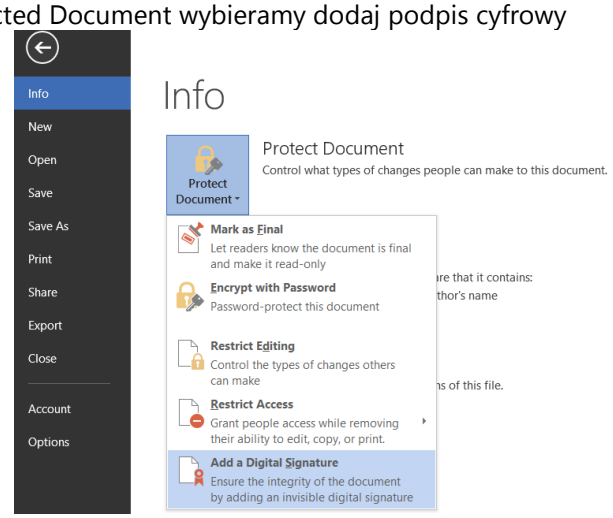
Podpis cyfrowy w Microsoft Office dostępny jest już od dość długie czasu jednak obsługa XAdES dostępna jest dopiero w wersji Office 2013. Możliwe jest podpisywanie dokumentów, arkuszy, formularzy InfoPath, wiadomości email czy nawet makr pisanych w VBA. Sposób obsługi przy pomocy graficznego interfejsu użytkownika jest prosty i nie wymaga specjalnej wiedzy, aby go używać.

Aby podpisać cyfrowo dokument w Microsoft Office możliwe są dwa sposoby:

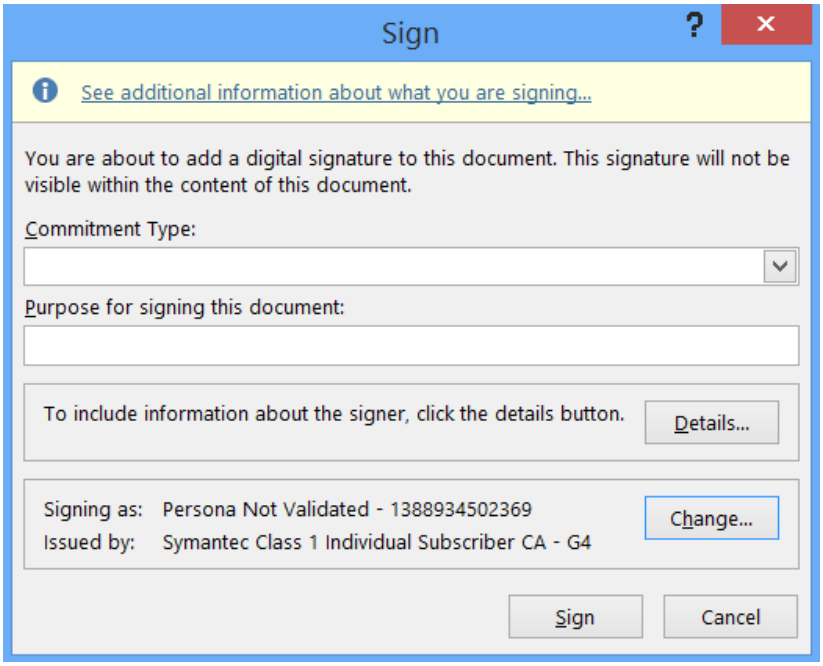
1. W naszym dokumencie wybieramy opcję Info



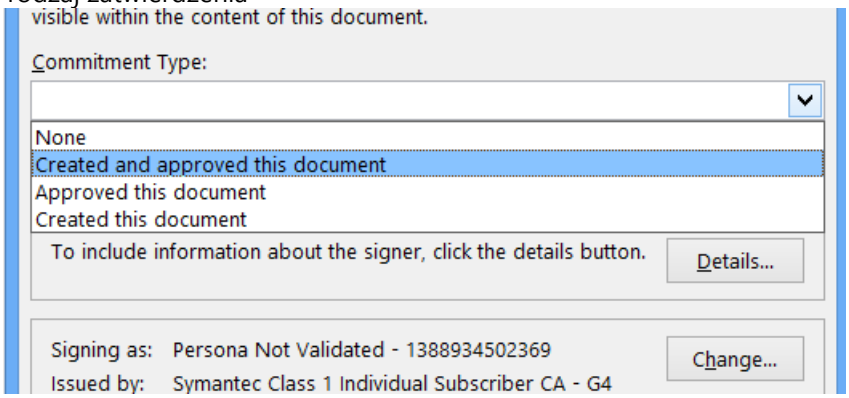
2. Z opcji Protected Document wybieramy dodaj podpis cyfrowy



3. Z opcji

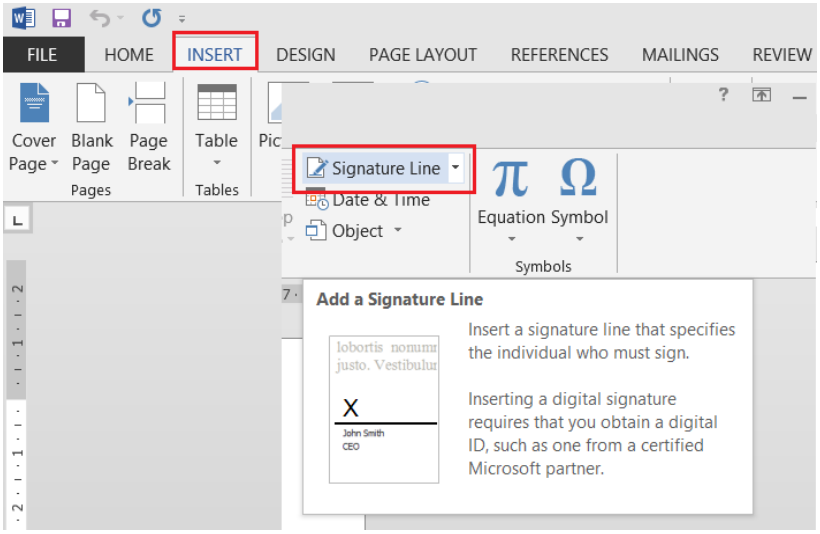


Wybieramy rodzaj zatwierdzenia

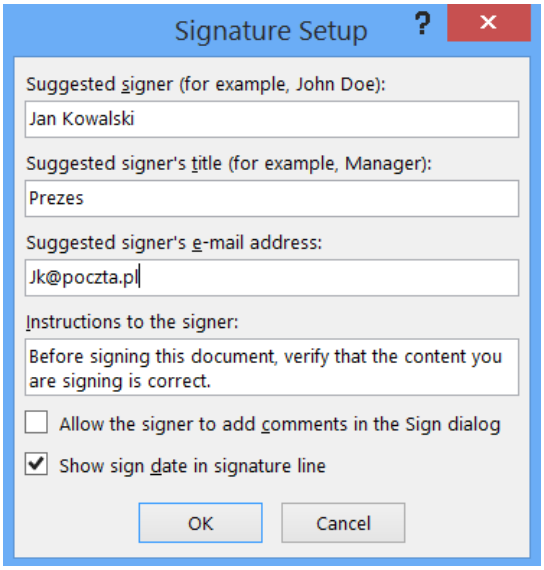


Oraz wpisujemy opis.

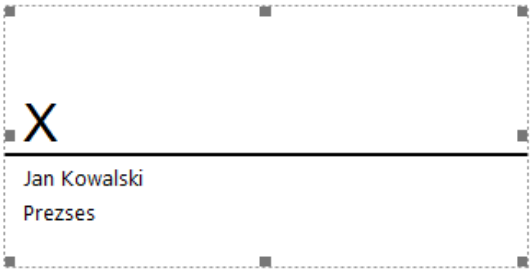
Drugi ze sposobów podpisania dokumentu to wybranie opcji „Podpis (Signature Line)” ze wstążki Wstaw



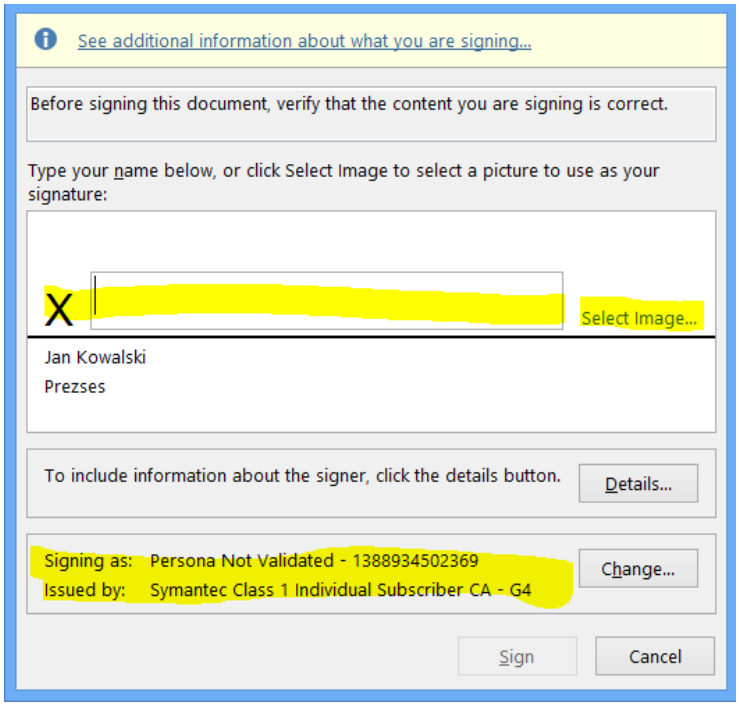
Następnie wypełniamy podstawowe dane o osobie podpisującej:



Pojawi się takie okno:

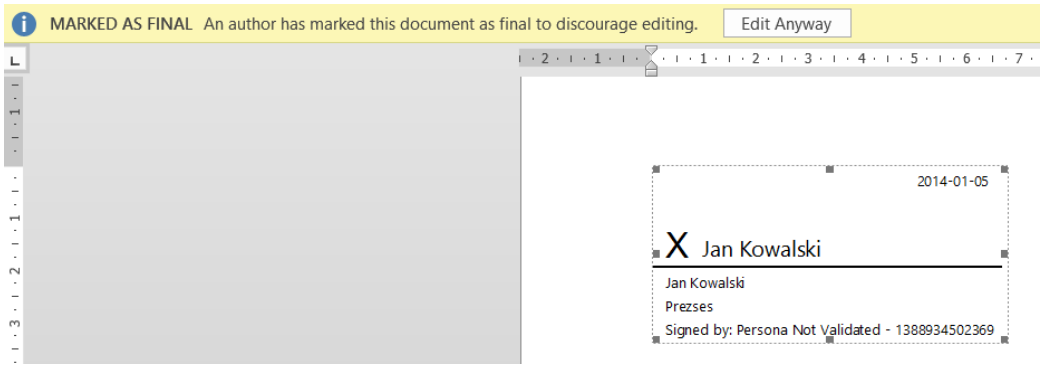


Dwukrotne kliknięcie na nim pozwoli na dodanie obrazka symbolizującego nasz podpis (tzw. faksymilia) lub po prostu wpisać swoje dane

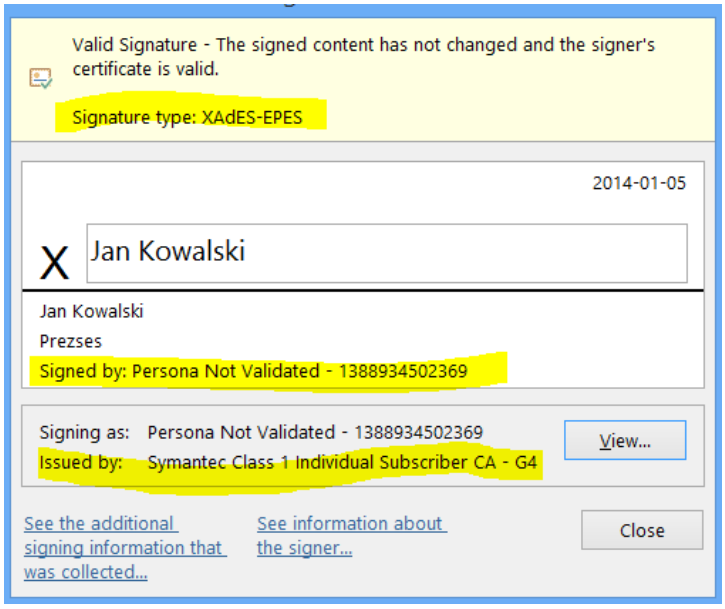


W dolnej części pokazany jest użyty certyfikat – możliwa jest jego zmiana.

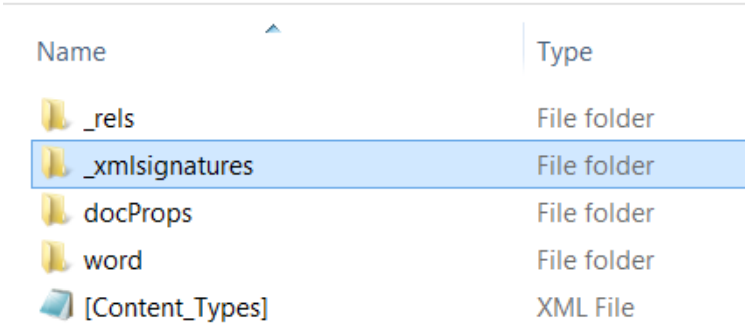
Po zaakceptowaniu podpisu nasz dokument zostaje podpisany – pojawia się belka informacyjna:



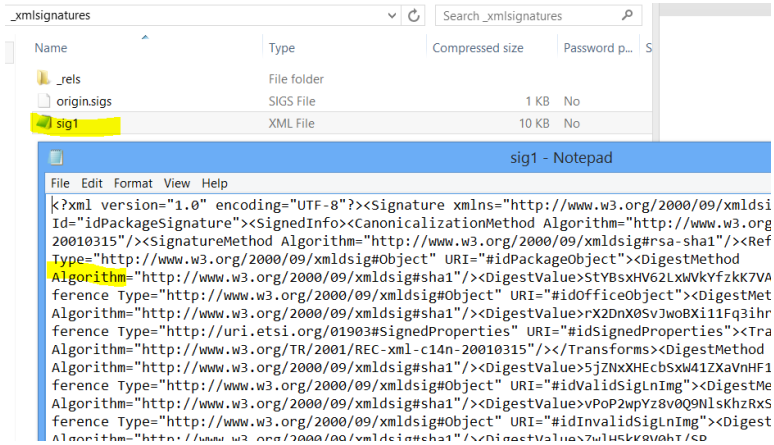
Dwukrotne kliknięcie na podpisie pokazuje typ podpisu XAdES, właściciela podpisu oraz możliwość walidacji tego podpisu (w przykładzie użyty jest testowy certyfikat dlatego właścicielem podpisu jest „Persona Not Validated”.



Po zapisaniu takiego dokumentu możemy zobaczyć jego strukturę (zamieniamy rozszerzenie docx na zip) i otwieramy archiwum. W strukturze pojawia się folder _xmlsignatures



Którego zawartość pokazuje certyfikat oraz informacje o podpisie



Każda zmiana pliku spowoduje usunięcie podpisu.

Office i podpis cyfrowy z punktu widzenia programisty

Po zapisaniu dokumentu w formacie Word mamy możliwość zobaczenia jak wygląda taki plik i gdzie dokładnie znajduje się nasz podpis. W momencie, gdy otworzymy zawartość naszego pliku od razu możemy zobaczyć katalog o nazwie *_xmlsignatures*. W folderze tym znajduje się plik z relacjami dla naszego podpisu *_rels* oraz plik sig1.xml – tu jest zapisany nasz pierwszy klucz – kluczy może być więcej niż jeden, dlatego pliki są numerowane. Jeśli przyjrzymy się jego strukturze to podstawowymi elementami są informacja o kluczu oraz informacja o podpisie.

Informacja o kluczu wygląda następująco i użytym certyfikacie (skrócona ze względu na długość) przedstawiona jest na listingu:

```
<SignatureValue>
      gUZ1Ed5T57Gs1q3IYUUN/OI5JrAHBCwaQPvC6tIxqyZPc6ZSML4TNeC5K7Yjjt
      7zoI8/eQRyHkDuDSX1ULStedSaw=
</SignatureValue>
<RSAKeyValue>
      <Modulus>
            vGgDwKmYLbyCIrP1qDYABfKcuC11Nd+pqxbogwdpye1pTQA2N4CQbLitBVmlb0
      </Modulus>
      <Exponent>AQAB</Exponent>
</RSAKeyValue>
<X509Data>
<X509Certificate>
      MIIBzTCCATagAwIBAgIQ6Tfat7ZSE6ZJA2IPfpGhFDANBgkqhkiG9w0BAwpnBIi6OXNagLOB69/rm
zHndgRWccUQl8W+NNH8od3PvCkOvjE0om0qeCDKdybR5hlML3GLZ
Ta1C6tKFNjYUQhuCfnxDm1YfLnWQ8Rg7HsWlNOhKGT1y
</X509Certificate>
</X509Data>
```

W dalszej części pliku możemy znaleźć informację o podpisie i jest to jednocześnie kluczowy element, który w dalszej części będziemy programować

```
<SignatureProperties>
  <SignatureProperty Id="idOfficeV1Details" Target="#idPackageSignature">
    <SignatureInfoV1 xmlns="http://schemas.microsoft.com/office/2006/digsig">
    <SetupID />
    <SignatureText />
    <SignatureImage />
    <SignatureComments>Test podpisu</SignatureComments>
    <WindowsVersion>6.0</WindowsVersion>
```

```
     <OfficeVersion>12.0</OfficeVersion>
    <ApplicationVersion>12.0</ApplicationVersion>
       <SignatureProviderId>
          {00000000-0000-0000-0000-000000000000}
       </SignatureProviderId>
    <SignatureProviderUrl />
          <SignatureProviderDetails>9</SignatureProviderDetails>
          <ManifestHashAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1
    </ManifestHashAlgorithm>
    <SignatureType>1</SignatureType>
    </SignatureInfoV1>
 </SignatureProperty>
</SignatureProperties>
```

Skąd taka struktura pliku? Podpis cyfrowy w dokumentach Office jest zgodny z podpisami XML – jako standard opisany przez W3C w dokumencie XML-Signature Syntax and Processing (http://www.w3.org/TR/xmldsig-core/). Struktura podpisu opisana jest w sposób następujący i jednocześnie tak jest implementowana w OpenXML jak przedstawia listing:

```
<Signature>
   <SignedInfo>
      (CanonicalizationMethod)
      (SignatureMethod)
      (<Reference(URI=)?>
      (Transforms)
      (DigestMethod)
      (DigestValue)
      </Reference>)+
      </SignedInfo>
      (SignatureValue)
      (KeyInfo)?
      (Object)*
</Signature>
```

Warto zwrócić uwagę na następujące elementy: *Reference* – każdy element, który ma być podpisany posada własny element *Reference* identyfikowany przez atrybut URI.

Transforms – specyfikuje listę kroków (kolejność) wykonania, które będą stosowane do obiektów opisanego przez *Reference*.
DigestValue – obiekt przechowuje wartość skrótu obiektu opisanego przez *Reference*.
SignatureValue – element przechowuje wartość zaszyfrowanego skrótu elementu *SignedInfo*.
KeyInfo – element wskazuje klucz do walidacji podpisu.

Open Packaging Convention specyfikuje model tworzenia pakietów oraz opisuje pakiety, części oraz relacje. Pakiety przechowuję części, które to przechowują zawartość oraz zasoby. Wsparcie dla programisty dla podpisywania pakietów zapewnia klasa dostępna w .NET Framework – *PackageDigitalSignatureManager*. Klasy specyficzne dla pakietów zdefiniowane są w przestrzeni nazw *System.IO.Packaging* a specyficzne do podpisywani cyfrowego w przestrzeni *System.Security.Cryptography.Xml*. Aplikacja definiuje listę części dokumentu, które można podpisać oraz wywołuje metodę *PackageDigitalSignatureManager.Sign()* do utworzenia podpisu i dodaje infrastrukturę podpisu do pakietu.

Aby podpisać dokument należy wykonać następujące kroki:
1. Należy utworzyć obiekt ***PackageDigitalSignatureManager***

```
// Otwieramy pakiet.
Package package = Package.Open(filename);


// Tworzymy obiekt PackageDigitalSignatureManager
  PackageDigitalSignatureManager dsm =
    new PackageDigitalSignatureManager(package);
```

2. Ustawiamy właściwości dla certyfikatu w utworzonym obiekcie ***PackageDigitalSignatureManager***

```
dsm.CertificateOption =
    CertificateEmbeddingOption.InSignaturePart;


     // gdzie opcjami mogą być
// InSignaturePart – certyfikat osadzony w podpisie.
// InCertificatePart – certyfikat osadzony w
//                     osobnej części.
```

3. Podpisanie listy części

```
//Inicjalizacja listy to trzymania URI do podpsiu.
System.Collections.Generic.List<Uri> partsToSign =
    new System.Collections.Generic.List<Uri>();


     //Dodanie każdej części do listy poza relacjami
```

```
    foreach (PackagePart packagePart in package.GetParts())
    {
        if (!PackUriHelper.IsRelationshipPartUri(packagePart.Uri))
      partsToSign.Add(packagePart.Uri);
    }
```

4. Utworzenie obiektu typu Certyfikat
   Aby użyć podpisu należy posiadać prawidłowy certyfikat X.509. W tym celu tworzymy obiekt klasy *System.Security.Cryptography.X509Certificates.X509Certificate2*, który jest parametrem metody *Sign()* obiektu typu *PackageDigitalSignatureManager*
   Dodatkowo możemy użyć klasy X509Store, aby pobrać dla aktualnego użytkownika certyfikat.

```
X509Store store = new X509Store(StoreLocation.CurrentUser);
store.Open(OpenFlags.OpenExistingOnly);
X509Certificate2Collection certificates = store.Certificates
    .Find(X509FindType.FindByKeyUsage, X509KeyUsageFlags.DigitalSignature, false)
    .Find(X509FindType.FindBySubjectName, keyName, false);
```

5. Stosujemy podpis
   Zastosowanie podpisu wymaga użycia metody *Sign()* oraz zamknięcia pakietu.

```
PackageDigitalSignature signature = dsm.Sign(partsToSign,
    x509Certificate, relationshipSelectors);
package.Close();
```

Weryfikacja podpisu i certyfikatu

Mając podpisany dokument należy zweryfikować jego poprawność. Najprostszym sposobem sprawdzenia czy nasz dokument został prawidłowo podpisany jest uruchomienie aplikacji, która obsługuje nasze dokumenty – na przykład Microsoft Word.
To jest oczywiście sposób, jeśli sami będziemy pracować z danym dokumentem. Co zrobić, jeśli napisaliśmy aplikację, która przetwarza dane z takich dokumentów? W tym przypadku również mamy możliwość użycia standardowych klas i metod. Obiekt klasy PackageDigitalSignature posiada właściwość Signer, która zwraca certyfikat służący do podpisania dokumentu.
Używając teraz metody VerifyCertificate() z klasy *PackageDigitalSignatureManager* możemy sprawdzić prawidłowość certyfikatu

```
if(PackageDigitalSignatureManager.VerifyCertificate(signature.Signer)
!= X509ChainStatusFlags.NoError)
{
// Application-specific code for error handling
// or certificate validation
}
```

SharePoint

Kwestie związane z bezpieczeństwem platformy SharePoint rozpoczynają się już w momencie jej wdrożenia. Istnieje zestaw najlepszych praktyk, które pokazują w jaki sposób zapewnić bezpieczne wdrożenie produktu.

Istnieje kilka najważniejszych punktów związanych z zabezpieczeniem instalacji SharePoint, należą do nich między innymi:

- Planowanie kont instalacyjnych
- Separacja danych
- Planowanie i uruchomienie Web Aplikacji
- Planowanie dostępu anonimowego
- Określenie kontroli dostępu do informacji
- Zabezpieczenie treści

Szczegółowy opis planowania znajduje się na Technet: http://technet.microsoft.com/en-us/library/hh377941.aspx

Planowanie kont instalacyjnych

Najistotniejszym elementem przy planowaniu wdrożenia SharePoint jest kwestia planowania kont, na których będą działać odpowiednie usługi oraz sposobie ich odzwierciedlenia w systemie.

Podstawowe zasady dla kont to między innymi:

- Wszystkie konta powinny być kontami Active Directory
- Konta nie powinny być kontami osobistymi, szczególnie dla Administratora Farmy
- Wszystkie konta zarządzane powinny mieć jeden centralny adres email, np. sharepointservice@company.com
- Każda Web Aplikacja powinna pracować na swoim dedykowanym koncie.

Planowanie kont można podzielić na trzy poziomy bezpieczeństwa (w zależności od potrzeb firmy):

- Niskie
- Średnie
- Wysokie

Plan kont użytkowników można zaprezentować w postaci tabeli z opisem dla poszczególnego konta. Szczegółowy opis dla poszczególnych kont znajduje się pod tabelami.

Niski poziom bezpieczeństwa

Nazwa	Opis	Uprawnienia lokalne	Uprawnienia domenowe
SQL Server			
SQL_Admin	Konto do uruchomienia usługi SQL Server. Na tym koncie uruchomione są następujące usługi SQL: • SQLSERVERAGENT • MSSQLSERVER	Lokalny administrator na serwerze SQL oraz SQL Admin na serwerze SQL.	Użytkownik domeny
SharePoint			
SP_Farm	Konto służące do wykonywania następujących czynności: • Instalacja produktu SharePoint • Konfiguracja farmy SharePoint • Konto zarządzane, na których uruchomiona jest pula aplikacji dla witryny administracji Centralnej • Uruchomienia usługi SharePoint Foundation Workflow Timer Service	Lokalny administrator na wszystkich serwerach SharePoint Security Admin oraz DB_Creator na instancji SQL Server, na której tworzone są bazy SharePoint	Użytkownik domeny
SP_Pool	Konto do uruchamiania pól aplikacji dla aplikacji web		Brak
SP_Services	Konto do uruchamiania usług aplikacji		Brak
SP_Crawl	Konto dla usługi wyszukiwanie służące do przeszukiwania i indeksowania treści		Brak
SP_UserProfiles	Konto potrzebne do uruchomienia usługi synchronizacji profili		Wymagane uprawnienia Replicating Directory Changes

Średni poziom bezpieczeństwa

Nazwa	Opis	Uprawnienia lokalne	Uprawnienia domenowe
SQL Server			
SQL_Admin	Konto administratora SQL Server. Służy również do instalacji serwera bazy danych.	Lokalny administrator na serwerze SQL oraz SQL Admin na serwerze SQL.	Użytkownik domeny
SQL_Services	Konto serwisowe - Na tym koncie uruchomione są następujące usługi SQL: • SQLSERVERAGENT • MSSQLSERVER		Brak
SharePoint			

SP_Farm	Konto służące do wykonywania następujących czynności: • Konfiguracja farmy SharePoint • Konto zarządzane, na których uruchomiona jest pula aplikacji dla witryny administracji Centralnej • Uruchomienia usługi SharePoint Foundation Workflow Timer Service	Lokalny administrator na wszystkich serwerach SharePoint Security Admin oraz DB_Creator na instancji SQL Server, na której tworzone są bazy SharePoint	Użytkownik domeny
SP_Admin	Konto służące do wykonania następujacych operacji adminsitracyjnych: • Instalacja produktu SharePoint • Uruchomienie kreatora konfiguracji	Lokalny administrator na wszystkich serwerach SharePoint Security Admin oraz DB_Creator na instancji SQL Server, na której tworzone są bazy SharePoint	Użytkownik domeny
SP_Pool	Konto do uruchamiania pól aplikacji dla aplikacji web		Brak
SP_Services	Konto do uruchamiania usług aplikacji		Brak
SP_Search	Konto uruchomienia usługi wyszukiwania		Brak
SP_Crawl	Konto dla usługi wyszukiwanie służące do przeszukiwania i indeksowania treści		Brak
SP_UserProfiles	Konto potrzebne do uruchomienia usługi synchronizacji profili		Wymagane uprawnienia Replicating Directory Changes

Wysoki poziom bezpieczeństwa

Nazwa	Opis	Uprawnienia lokalne	Uprawnienia domenowe
SQL Server			
SQL_Admin	Konto administratora SQL Server. Służy również do instalacji serwera bazy danych.	Lokalny administrator na serwerze SQL oraz SQL Admin na serwerze SQL.	Użytkownik domeny
SQL_Agent	Konto do uruchomienia usługi SQLSERVERAGENT		Brak
SQL_Engine	Konto serwisowe do uruchomienia usługi MSSQLSERVER		Brak
SharePoint			
SP_Farm	Konto służące do wykonywania następujących czynności: Konfiguracja farmy SharePoint	Lokalny administrator na wszystkich serwerach SharePoint Security Admin oraz	Użytkownik domeny

	Konto zarządzane, na których uruchomiona jest pula aplikacji dla witryny administracji Centralnej Uruchomienia usługi SharePoint Foundation Workflow Timer Service	DB_Creator na instancji SQL Server, na której tworzone są bazy SharePoint	
SP_Admin	Konto służące do wykonania następujacych operacji adminsitracyjnych: • Instalacja produktu SharePoint • Uruchomienie kreatora konfiguracji	Lokalny administrator na wszystkich serwerach SharePoint Security Admin oraz DB_Creator na instancji SQL Server, na której tworzone są bazy SharePoint	Użytkownik domeny
SP_Pool	Konto do uruchamiania pól aplikacji dla aplikacji web		Brak
SP_Services	Konto do uruchamiania usług aplikacji		Brak
SP_Search	Konto uruchomienia usługi wyszukiwania		Brak
SP_Crawl	Konto dla usługi wyszukiwanie służące do przeszukiwania i indeksowania treści		Brak
SP_UserProfiles	Konto potrzebne do uruchomienia usługi synchronizacji profili		Wymagane uprawnienia Replicating Directory Changes
Sp_MySitePool	Używane do uruchomienia obsługi Witryn Osobistych		Brak

Objaśnienia dla poszczególnych kont serwisowych

SQL_Admin – jest to główne konto administratora SQL Server. Konto to wymaga uprawnień lokalnego administratora, tak aby możliwe było wykonanie operacji instalacji bazy SQL.

SQL_Agent – konto to nie posiada żadnych lokalnych uprawnień. Jest używane tylko i wyłączenie do uruchomienia usługi Windows SQL Agent.

SQL_Engine - konto to nie posiada żadnych lokalnych uprawnień. Jest używane tylko i wyłączenie do uruchomienia usługi Windows silnika bazy danych.

SP_Farm – jest to główne konto dla SharePoint. Musi posiadać uprawnienia lokalnego administratora na każdym serwerze w famie SharePoint, aby możliwe było zainstalowanie i skonfigurowanie SharePoint. Musi posiadać również na czas instalacji role securityadmin oraz dbcreator w bazie SQL Server aby możliwe było utworzenie odpowiednich baz danych. Konto to będzie odpowiadało za usługi czasomierza SharePoint oraz aplikacji web Administracja Centralna.

SP_Admin – jest kontem domenowym, które służy tylko i wyłącznie do instalacji i konfiguracji farmy. Dodatkowo za jego pomocą uruchamiany jest kreator konfiguracji SharePoint (o ile jest używany kreator). Musi posiadać uprawnienia lokalnego administratora na każdym serwerze w famie SharePoint.

SP_Pool – konto domenowe dla identyfikowania każdej z utworzonych pól aplikacyjnych. Każda Web Aplikacja powinna mieć swoją pulą aplikacyjną uruchomioną na odrębnym koncie.

SP_Service – konto służące do uruchamiania poszczególnych usług, przykładowo usługa synchronizacji profili. Przykładowa lista kont:

- SP.Cache
- SP.CacheReader
- SP.C2WTSAccount
- SP.UPSAService
- SP.MMService
- SP.SSOService
- SP.SubScriptionS
- SP.BDCService
- SP.APPManService

SP_Crawl – konto to jest używane przez usługę wyszukiwania. W ramach tej usługi konto to przeszukuje treść i buduje indeks. W związku z tym konto to musi posiadać uprawnienia do czytania wszelkich treści, które są podłączone do usługi wyszukiwania.

SP_Search – służy do uruchomienia usługi SharePoint Windows Search Service.

SP_UserProfiles – konto to używane jest do synchronizacji pomiędzy usługą profili w SharePoint a Active Directory. Konto to nie potrzebuje żadnych praw lokalnych, jednak trzeba nadać mu uprawnienia replikacji zmian katalogu w usłudze Active Directory w celu umożliwienia synchronizacji.

SP_MySitePool – jest kontem domenowym, na którym działa pula aplikacji dla usługi witryn osobistych. Jest bardzo podobne do konta SP_Pool, ale dedykowane usłudze Witryny Osobiste.

Dostęp anonimowy

Platforma SharePoint bardzo często jest używana do publikacji treści dla użytkowników anonimowych, szczególnie jeśli nasz serwer jest wystawiony do publicznego wglądu w Internecie.

W takim przypadku największym zagrożeniem i ryzykiem jest nieumyślne udostępnianie danych na publicznej stronie WWW.

Warto zwrócić uwagę, że wszystkie witryny formularzy oraz web serwisów są dostępne publicznie (!!) i na to szczególnie należy zwrócić uwagę.

Poniżej znajduje się lista adresów, na które należy zwrócić szczególną uwagę:

- /_layouts/adminrecyclebin.aspx – ustawienia witryny kosz
- /_layouts/bpcf.aspx - Nowa strona podstawowa
- /_layouts/create.aspx – Utwórz nowy element
- /_layouts/listfeed.aspx – RSS feed dla listy
- /_layouts/managefeatures.aspx – zarządzanie funkcjami witryny
- /_layouts/mngsiteadmin.aspx – Administratorzy zbioru witryn
- /_layouts/mngsubwebs.aspx – Lista witryn I obszarów roboczych
- /_layouts/policy.aspx – Zasady dla witryny

- /_layouts/policyconfig.aspx – Edytowanie zasad
- /_layouts/policylist.aspx - strona służy do tworzenia i modyfikowania zasad zarządzania informacjami w danym zbiorze witryn.
- /_layouts/mcontent.aspx – strona prezentująca biblioteki i listy witryny
- /_layouts/storman.aspx - strona zawiera informacje o alokacji przydziału w witrynie
- /_layouts/recyclebin.aspx – kosz strony. Tutaj przechowywane są skasowane informacje ze strony
- /_layouts/wrkmng.aspx - Przepływy pracy w bieżącym zbiorze witryn
- /_layouts/vsubwebs.aspx - Na tej stronie są pokazywane wszystkie witryny sieci Web utworzone pod danym adresem. Adresy URL przedstawiają hierarchię różnych witryn.
- /_layouts/pagesettings.aspx – ustawienia wybranej strony
- /_layouts/settings.aspx – strona "Ustawienia witryny"
- /_layouts/newsbweb.aspx – strona pozwalająca na utworzenie nowej witryny programu SharePoint
- /_layouts/userdisp.aspx – strona prezentująca informacje o użytkowniku
- /_vti_bin/ - tutaj znajdują się web serwisy SharePoint

Standardowo po wpisaniu któregoś z tych adresów pojawi się błąd http lub okno logowania. Taka sytuacja może doprowadzić do próby włamania.

W celu zabezpieczenia dostępu do stron dostępnych pod adresem /_layouts oraz Web Serwisów należy odpowiednio zmodyfikować web.config – do pliku web.config należy wprowadzić następujące sekcje:

```
<add path="configuration">
  <location path="_layouts">
    <system.web>
      <authorization>
        <deny users="?" />
      </authorization>
    </system.web>
  </location>
```

```
<location path="_vti_bin">
  <system.web>
    <authorization>
      <deny users="?" />
    </authorization>
  </system.web>
</location>
```

```
<location path="_loyouts/login.aspx">
  <system.web>
    <authorization>
      <allow users="?" />
    </authorization>
```

```
  </system.web>
</location>
```

```
<location path="_loyouts/error.aspx">
  <system.web>
    <authorization>
      <allow users="?" />
    </authorization>
  </system.web>
</location>
```

```
<location path="_loyouts/accessdenied.aspx">
  <system.web>
    <authorization>
      <allow users="?" />
    </authorization>
  </system.web>
</location>
```

W przypadku dostępu anonimowego warto rozważyć jeszcze następujące zasady bezpieczeństwa:

1. Usunięcie wszelkich uprawnień przeglądania stron aplikacyjnych (konfiguracyjnych)
2. Dla wszystkich użytkowników anonimowych dać uprawnieninia Dostęp Ograniczony (Limited Access)
3. Włączenie funkcji Lockdown, która działa na witrynie publikowania. Dzięki temu możemy zablokować dostęp do stron formularzy, np. /Pages/Forms/AllItems.aspx

Aby włączyć funkcję Lockdown należy wykonać następujące czynności:

1. Sprawdzamy czy funkcjonalność jest zainstalowana
   Get-SPFeature –site http://portal

2. Jeśli funkcjonalność nie jest dostępna należy ją włączyć:
   Stsadm –o activatefeature –url –filename ViewFormPagesLockDown\feature.xml

3. Aby ją wyłączyć można użyć polecenia:
   Stsadm –o deactivatefeature –url –filename ViewFormPagesLockDown\feature.xml

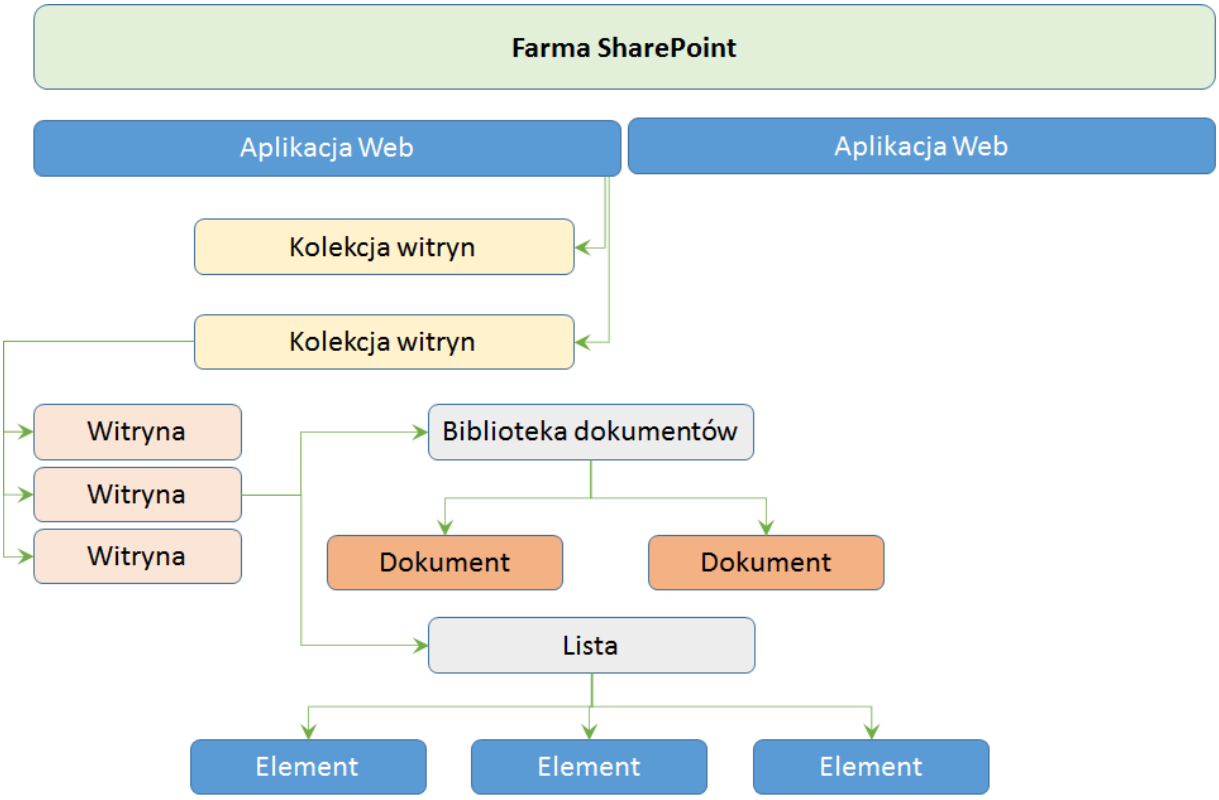
Uprawnienia w SharePoint

Planując wdrożenie SharePoint należy zwrócić szczególną uwagę na planowanie uprawnień dla użytkowników oraz zapoznać się z tym jak wyglądają uprawnienia w SharePoint i jak z nimi pracować.

Na początek należy zwrócić uwagę, że w SharePoint model uprawnień jest hierarchiczny oznacza to, że poszczególne uprawnienia są dziedziczone w ramach witryny dla poszczególnych obiektów. Domyślnie jest włączone dziedziczenie uprawnień

Istnieje możliwość przerwania dziedziczenia na dowolnym poziomie i zarządzania nimi niezależnie.

Struktura hierarchiczna obiektów w SharePoint przedstawia się następująco:



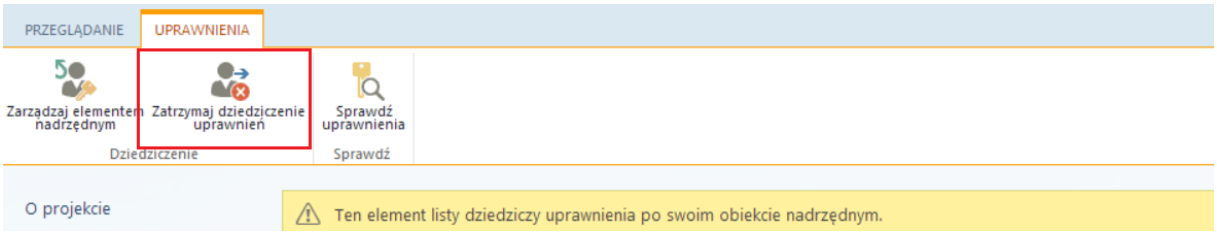
Gdzie na poziomie kolekcji witryn automatycznie tworzone są grupy uprawnień:

- Właściciele kolekcji witryn
- Członkowie kolekcji witryn
- Odwiedzający kolekcję witryn

Grupy te są grupami SharePoint, ale możliwe jest przypisanie również grup Active Directory oraz pojedynczych użytkowników. Patrząc na rysunek możliwe jest stworzenie takich uprawnień tak, aby na każdym poziomie (zaczynając od kolekcji witryn a kończąc na poszczególnych elementach) uprawnienia były unikatowe.

Standardowe grupy uprawnień po utworzeniu witryny mogą wyglądać następująco:

Dowolny obiekt w kolekcji witryn może mieć niezależny zestaw uprawnień – możliwe jest to przez zatrzymanie dziedziczenia uprawnień:



Przerywając dziedziczenie na danym poziomie w momencie, w którym tworzone są unikatowe uprawnienia dla elementu SharePoint automatycznie tworzy hierarchię uprawnień dla elementów podrzędnych oraz tworzy uprawnienie o nazwie „Dostęp ograniczony". Celem tworzenia takowego uprawnienia jest umożliwienie użytkownikowi minimalny zestaw uprawnień do nawigacji do danego elementu (nawet jeśli nie mieliśmy wcześniej dostępu do folderu, biblioteki lub witryny).

Wyzwaniem dla administratora, związanym z uprawnieniem „Ograniczony Dostęp", jest to, że nigdy nie jest automatycznie usuwany lub czyszczony wtedy, gdy dany obiekt ponownie dziedziczy uprawnienia po obiekcie nadrzędnym. Należy na bieżąco monitorować ile jest uprawnień tego typu, ponieważ wpływa to na ogólną liczbę uprawnień a co za tym idzie możemy szybko osiągnąć limit ilości unikatowych uprawnień.

Limity

Limit	**Wartość maksymalna**	**Typ limitu**	**Opis**
Ilość grup SharePoint, do których może należeć użytkownik	5,000	Wsparcie	Nie jest to twarde ograniczenie ale wynika ze wskazówek projektowanie Active Directory. Czynniki wpływające na tą liczbę: • Wielkość tokenu użytkownika • Cache dla grup: SharePoint 2013 zawiera tabelę, która przechowuje liczbę grup, do których należy użytkownik. • Czas sprawdzenia uprawnień użytkownika w grupie dla danego obiektu wzrasta wraz z liczbą grup, do których należy użytkownik
Użytkowników w kolekcji witryn	2 miliony dla kolekcji witryn	Wsparcie	Można dodać dowolną liczbę użytkowników do witryny korzystając z grup bezpieczeństwa Windows zamiast dodawania pojedynczych użytkowników.

			Ograniczenie wynika z łatwości zarządzania I nawigacji w interfejsie użytkownika. W przypadku posiadania dużej liczby użytkowników lub grup w kolekcji witryn należy użyć PowerShell do zarządzania użytkownikami zamiast klasycznego interfejsu użytkownika.
Użytkowników AD w grupie SharePoint	5,000 na grupę SharePoint	Wsparcie	SharePoint Server 2013 pozwala na dodanie użytkowników lub grup AD do grupy SharePoint. Po dodaniu więcej niż 5000 elementów do grupy nastąpi spadek wydajności system przy weryfikowaniu uprawnień oraz wyświetlania osób w widoku.
Ilość grup SharePoint	10,000 w kolekcji witryn	Wsparcie	Powyżej 10000 grup czas wykonania operacji drastycznie wzrasta. Szczególnie trudne wtedy staje się dodanie nowej osoby do grupy, stworzenie nowej grupy czy wyświetlenie zawartości grupy.

Poziomy uprawnień

Ważną cechą w zarządzaniu uprawnieniami w SharePoint jest możliwość tworzenia swoich własnych poziomów uprawnień. Standardowo system tworzy następujące poziomy uprawnień:

- *Pełna kontrola* - Ma pełną kontrolę.
- *Projektowanie* - Może przeglądać, dodawać, aktualizować, usuwać, zatwierdzać i dostosowywać.
- *Edycja* - Może dodawać, edytować i usuwać listy, jak również przeglądać, dodawać, aktualizować i usuwać elementy listy i dokumenty.
- *Współtworzenie* - Może przeglądać, dodawać, aktualizować i usuwać elementy listy i dokumenty.
- *Czytanie* - Może wyświetlać strony i elementy list oraz pobierać dokumenty.
- *Ograniczony dostęp* - Może przeglądać określone listy, biblioteki dokumentów, elementy listy, foldery oraz dokumenty po nadaniu uprawnień.
- *Zatwierdzanie* - Może edytować i zatwierdzać strony, elementy listy oraz dokumenty.
- *Zarządzanie hierarchią* - Może tworzyć witryny i edytować strony, elementy listy oraz dokumenty.
- *Odczyt z ograniczeniami* - Może wyświetlać strony i dokumenty, nie ma jednak dostępu do ich wersji historycznych ani do uprawnień użytkownika.
- *Ograniczone interfejsy tłumaczeń* - Nie można otwierać list i folderów ani korzystać z interfejsów zdalnych.
- *Umiarkowane* - Może wyświetlać, dodawać, aktualizować, usuwać i moderować elementy listy i dokumenty
- *Tylko przeglądanie* - Może wyświetlać strony, elementy list oraz dokumenty. Typy dokumentów z dostępnymi programami obsługi plików na serwerze mogą być wyświetlane w przeglądarce, ale nie mogą być pobierane.

Istnieje możliwość stworzenie swojego własnego poziomu uprawnień a następnie przypisana go wybranym grupom użytkowników lub samym użytkownikom. Wśród dostępnych uprawnień mamy do dyspozycji między innymi:

Uprawnienia listy

- Zarządzanie listami - Tworzenie lub usuwanie list, dodawanie lub usuwanie kolumn list albo dodawanie lub usuwanie widoków publicznych list.
- Zastępowanie zachowań list - Odrzucanie lub ewidencjonowanie dokumentu wyewidencjonowanego dla innego użytkownika oraz zmienianie lub zastępowanie ustawień pozwalających użytkownikom czytać/edytować tylko własne elementy
- Dodawanie elementów - Dodawanie elementów do list i dokumentów do bibliotek dokumentów.
- Edytowanie elementów - Edytowanie elementów na listach i dokumentów w bibliotekach dokumentów oraz dostosowywanie stron składników Web Part w bibliotekach dokumentów.
- Usuwanie elementów - Usuwanie elementów z listy i dokumentów z biblioteki dokumentów.
- Wyświetlanie elementów - Wyświetlanie elementów list i dokumentów w bibliotekach dokumentów.
- Zatwierdzanie elementów - Zatwierdzanie wersji pomocniczej elementu listy lub dokumentu.
- Otwieranie elementów - Wyświetlanie źródeł dokumentów za pomocą programów obsługi plików na serwerze.
- Wyświetlanie wersji - Wyświetlanie poprzednich wersji elementu listy lub dokumentu.
- Usuwanie wersji - Usuwanie poprzednich wersji elementu listy lub dokumentu.
- Tworzenie alertów - Tworzenie alertów.
- Wyświetlanie stron aplikacji - Wyświetlanie formularzy, widoków i stron aplikacji. Wyliczanie list.

Uprawnienia witryny

- Zarządzanie uprawnieniami - Tworzenie lub zmienianie poziomów uprawnień w witrynie sieci Web oraz przypisywanie uprawnień użytkownikom i grupom.
- Wyświetlanie danych funkcji Web Analytics - Wyświetlanie raportów dotyczących użycia witryny sieci Web.
- Tworzenie witryn podrzędnych - Tworzenie witryn podrzędnych, takich jak witryny zespołu, witryny obszarów roboczych spotkania oraz witryny obszarów roboczych dokumentu.
- Zarządzanie witryną sieci Web - Możliwość wykonywania wszystkich zadań administracyjnych dla witryny sieci Web oraz zarządzania zawartością.
- Dodawanie i dostosowywanie stron - Dodawanie, zmienianie lub usuwanie stron HTML bądź stron składników Web Part oraz edytowanie witryny sieci Web za pomocą edytora zgodnego z programem Microsoft SharePoint Foundation.
- Stosowanie motywów i obramowań - Stosowanie motywów lub obramowań w całej witrynie sieci Web.
- Stosowanie arkuszy stylów - Stosowanie arkuszy stylów (pliku CSS) w witrynie sieci Web.
- Tworzenie grup - Tworzenie grup użytkowników, których można używać w całym zbiorze witryn.
- Przeglądanie katalogów - Wyliczanie plików i folderów w witrynie sieci Web przy użyciu interfejsów programu SharePoint Designer i protokołu WebDAV.
- Używanie samoobsługowego tworzenia witryn - Tworzenie witryny za pomocą usługi samoobsługowego tworzenia witryn.

- Wyświetlanie stron - Wyświetlanie stron w witrynie sieci Web.
- Wyliczanie uprawnień - Wyliczanie uprawnień dla witryny sieci Web, listy, folderu, dokumentu lub elementu listy.
- Przeglądanie informacji o użytkownikach - Wyświetlanie informacji o użytkownikach witryny sieci Web.
- Zarządzanie alertami - Zarządzanie alertami dla wszystkich użytkowników witryny sieci Web.
- Używanie interfejsów zdalnych - Uzyskiwanie dostępu do witryny sieci Web przy użyciu interfejsów protokołów SOAP, WebDAV, modelu obiektów klienta oraz programu SharePoint Designer.
- Używanie funkcji integracji klienta - Używanie funkcji uruchamiających aplikacje klienckie. Bez tego uprawnienia użytkownicy będą musieli pracować nad dokumentami lokalnie, a następnie przekazywać wprowadzone zmiany.
- Otwieranie - Umożliwia użytkownikom otwieranie witryny sieci Web, listy lub folderu w celu uzyskania dostępu do elementów wewnątrz danego kontenera.
- Edytowanie informacji osobistych użytkownika - Umożliwia użytkownikowi zmianę własnych danych, na przykład dodanie obrazu.

Uprawnienia osobiste

- Zarządzanie widokami osobistymi - Tworzenie, zmienianie lub usuwanie widoków osobistych list.
- Dodawanie/usuwanie prywatnych składników Web Part - Dodawanie lub usuwanie prywatnych składników Web Part na stronach składników Web Part.
- Aktualizowanie osobistych składników Web Part - Aktualizowanie składników Web Part do wyświetlania informacji spersonalizowanych.

Ważne - podczas tworzenia nowego poziomu uprawnień system sam automatycznie wybiera te uprawnienia, które sią konieczne w zależności od tego jakie inne uprawnienie wybierzemy. Przykładowo dodając do listy uprawnień możliwość Edycji system automatycznie doda uprawnienie Wyświetlanie elementu.

Następnie tworząc grupę SharePoint możemy skorzystać ze stworzonych poziomów uprawnień:

Uwierzytelnianie w SharePoint

Microsoft SharePoint 2013 wyposażony jest w kilka opcji uwierzytelniania aby można go było łatwo dostosować do potrzeb organizacji. Proces uwierzytelnienia może być postrzegany jako proces weryfikacji tożsamości użytkownika względem dostawcy tożsamości. Dostawcami tożsamości dla SharePoint mogą być między innymi: Usługi katalogowe Active Directory (ADDS) lub Active Directory Federation Services (AD FS).

W SharePoint Server możliwe jest skonfigurowanie dostawcy tożsamości na poziomie pojedynczej aplikacji Web – każda z nich może opierać się o inny sposób autentykacji użytkowników. W trakcie tworzenia takiej aplikacji web do wyboru sposobu autoryzacji używa się konsoli dostępnej w Administracji Centralnej. Po utworzeniu witryny nie ma możliwości zmiany sposobu uwierzytelniania z poziomu Administracji Centralnej, ale tylko za pomocą komend PowerShell.

W SharePoint Portal Server 2013 istnieją cztery sposoby uwierzytelniania w portalu:

1. Autentykacja anonimowa
2. Autentykacja klasyczna Windows
3. Autentykacja oparta o formularze
4. Autentykacja oparta na Claims (SAML)

Autentykacja anonimowa

SharePoint 2013 wspiera dostęp anonimowy do portalu. Scenariusz taki najczęściej stosuje się przy publicznym udostępnianiu portalu użytkownikom w Internecie.

Standardowo mechanizm ten jest wyłączony. Aby go włączyć należy dla każdej Web Aplikacji, która ma być udostępniona włączyć w ustawieniach dostęp anonimowy

Uwierzytelnienie klasyczne Windows

SharePoint oferuje wiele opcji uwierzytelniania. Dwoma najpopularniejszymi wyborami dla organizacji w scenariuszach intranetowych są NTLM oraz Kerberos. Oba protokoły wykorzystywane są przy zintegrowanym uwierzytelnianiu systemu Windows. NTLM opiera się na wygenerowaniu przez IIS tokenu z żądaniem, wysłaniu go do klienta, odpowiedzi klienta tokenem i zweryfikowaniu odpowiedzi przez kontroler domeny. NTLM wymaga zaszyfrowania nazw użytkowników i haseł zanim zostaną przesłane oraz ponownego uwierzytelniania (nowego tokenu) podczas uzyskiwania dostępu do zasobu sieciowego. Z kolei Kerberos opiera się na systemie tokenów, gdzie klient i serwer uzyskują dostęp do zaufanego wystawcy jakim jest Centrum Dystrybucji Kluczy (KDC), które odpowiada na żądania klienta i przyznaje tokeny, za pomocą których klient może uzyskać dostęp do zasobów sieciowych. Kerberos nie wymaga ponownego uwierzytelniania dla uzyskania dostępu do wielu zasobów.

Jest wiele powodów, dla których warto korzystać z protokołu Kerberos lecz w większości przypadków będzie to wydajność lub bezpieczeństwo. Gdy zwiększa się obciążenie użytkownika lub złożoność topologii, NTML może powodować problemy związane z wydajnością, ponieważ uwierzytelnianie oparte na NTML z założenia wymaga wielu rund pomiędzy IIS a kontrolerem domeny.

Bardzo ważnym punktem w decyzji co do wyboru sposobu autentykacji jest np. użycie Office Web Apps, które nie wspierają standardowego sposobu uwierzytelniania i wymagają uwierzytelnienia opartego na bazie oświadczeń - (*claims-based authorization*).

Uwierzytelnienie oparte o formularze

Z uwierzytelnieniem opartym o formularze mamy najczęściej do czynienia przy witrynach WWW, gdzie użytkownik nie ma dostępu do Active Directory i jest zwykle użytkownikiem zewnętrznym.

Uwierzytelnienie oparte o formularze bazuje na dostawcy *ASP.NET mebership and role provider*, czyli mechanizmowi technologii ASP.NET do zarządzania logowaniem użytkowników. Użytkownik wprowadza nazwę oraz hasło a następnie jest autoryzowany w zewnętrznym źródle danych, np. bazie danych SQL, dowolnym LDAP jak również może być autoryzowany w Active Directory. Autoryzacja ta używa również Claims do poświadczeń.

Autentykacja oparta na bazie oświadczeń - (*claims-based authorization*)(SAML)

Microsoft wprowadził autentykację opartą na Claims już w SharePoint 2010. Dzięki temu możliwe było wsparcie różnych heterogenicznych dostawców uwierzytelnienia dostępnych w Internecie, np. Microsoft Account (dawne LiveID), OpenID, czy dowolny inny system autoryzacyjny.

Dzięki uwierzytelnieniu opartemu o Claims użytkownik po uwierzytelnieniu otrzymuje podpisany cyfrowo token od zaufanego dostawcy tożsamości. Token zawiera zestaw atrybutów a każdy Claim stanowi specyficzny zestaw danych na temat użytkownika. Za ten model autentykacji w SharePoint odpowiada usługa SharePoint Security Token Service (STS).

W SharePoint 2013 jest to podstawowy model autentykacji użytkownika.

Dodatkowe elementy bezpieczeństwa

Planując wdrożenie platformy SharePoint warto zwrócić uwagę również na dodatkowe elementy, które mogą wspomóc zapewnienie bezpieczeństwa platformy

Wyłączenie widoku Explorera Windows

W celu ochrony czułych danych w SharePoint wato rozważyć wyłączenie widoku Explorera Windows w SharePoint. Są co najmniej dwa powody do tego:

- Wielu użytkowników kopiuje lub przenosi pliki i foldery poprzez okno explorera
- Jest to jedyny sposób na skopiowanie jednocześnie kilku folderów do biblioteki SharePoint

Problemy wynikające z użycia tego trybu to między innymi fakt, że pomimo uprawnień tylko do odczytu użytkownik w tym trybie będzie mógł modyfikować nazwy plików. W niektórych przypadkach pomimo trybu tylko do odczytu użytkownik ma możliwość nawet skasowania pliku.

Użycie RMS

Każda firma bez względu na wielkość boryka się z ochroną informacji, do których to zaliczyć możemy wszelkie dokumenty firmowe oraz pocztę elektroniczną. Co zatem jesteśmy w stanie zrobić, aby chronić tajemnicę firmy? Najbardziej rozpowszechnionym sposobem zabezpieczenia informacji w firmie jest zastosowanie dwóch usług. Są to Windows Rights Management Services oraz Information Rights Management.

Windows Rights Management Services (RMS) to usługi systemu Windows Server, pozwalające aplikacjom obsługującym zarządzanie prawami definiować i egzekwować uprawnienia przypisane do informacji. Information Rights Management (IRM) jest rozszerzeniem usługi Windows Rights Management (RM) na aplikacje pakietu Microsoft Office. Aby skorzystać z IRM należy uruchomić RMS na platformie Windows Server lub skorzystać z usługi dostarczaną przez firmę Microsoft. IRM pozwala

dowolnym użytkownikom na określanie uprawnień dostępu do wiadomości e-mail oraz sposobu dostępu do dokumentów. Dzięki użyciu IRM mamy możliwość zapobiec drukowaniu, przesyłaniu dalej i kopiowaniu poufnych informacji przez osoby nieupoważnione.

Wiadomości email możemy zabezpieczyć przed kopiowaniem, przekazywaniem i drukowaniem. Jeśli dana wiadomość zostanie zabezpieczona to odpowiedni przyciski w programie zostaną zablokowane i nie będzie możliwości ich użycia. Bardzo ważną funkcjonalnością IRM jest zapewnienie bezpieczeństwa również załącznikom dla wiadomości pocztowych (pod warunkiem, że będą to dokumenty utworzone przy pomocy programów pakietu Office).

W przypadku samych dokumentów Office IRM pozwala na ochronę ważnych informacji biznesowych, takich jak np. raporty finansowe. Istnieje możliwość ustawienia zasad pozwalających ściśle kontrolować dostęp do danych tzn., kto może otwierać, kopiować, drukować bądź przesyłać informacje zawarte w dokumentach.

W wszelkich rozważaniach na temat ochrony informacji w firmie należy wziąć pod uwagę również inne sposoby pozyskania informacji. W takich przypadkach IRM (oraz inne systemy) nie są w stanie zabezpieczyć danych. Do takich przypadków zaliczyć możemy utratę danych w wyniku działania wirusów, robienie zdjęć, kopiowanie danych przy pomocy programów służących do przechwytywania zawartości ekranu.

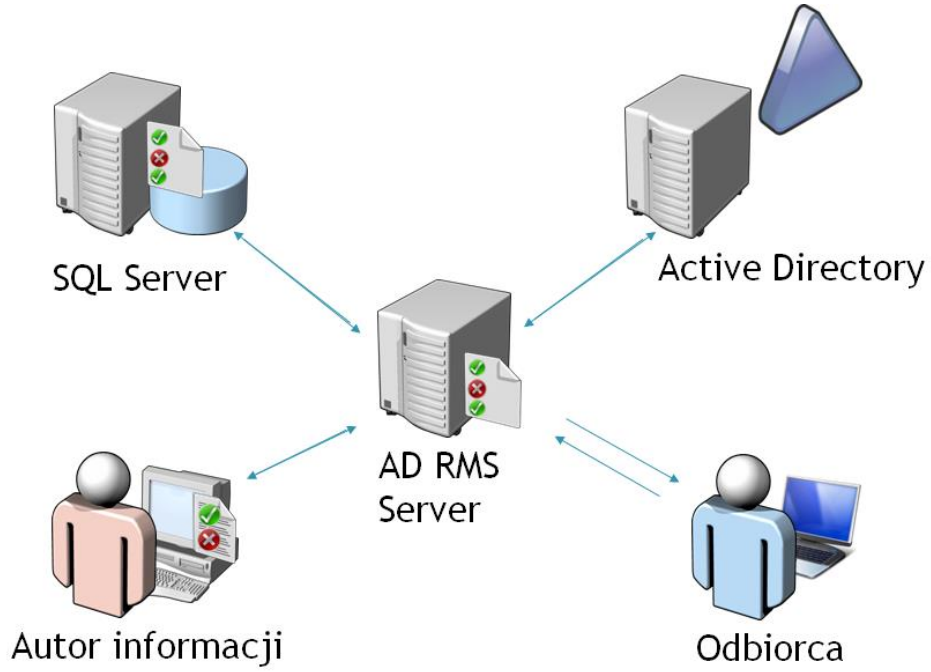
Proces korzystania z IRM składa się z trzech podstawowych kroków:

- Tworzenie – autor tworzy dokument, po czym nadaje odpowiednie uprawnienia da odpowiednich osób.
- Dystrybucja – czyli rozpowszechnienie pliku przez autora.
- Korzystanie –Odbiorca otwiera dokument w zwyczajny sposób. Podczas tej czynności aplikacja komunikuje się w tle z serwerem RMS, ustalając, czy dany użytkownik posiada prawa dostępu do pliku. RMS sprawdza użytkownika i wydaje zezwolenie na wykorzystanie dokumentu.

Technologia, która stoi za RMS i IRM to platforma programistyczna .NET Framework wraz z XrML (Extensible Rights Markup Language). XrML oparty jest na standardzie XML. Połączenie tych dwóch technologii pozwala na tworzenie własnych rozwiązań korzystających z RMS oraz IRM.

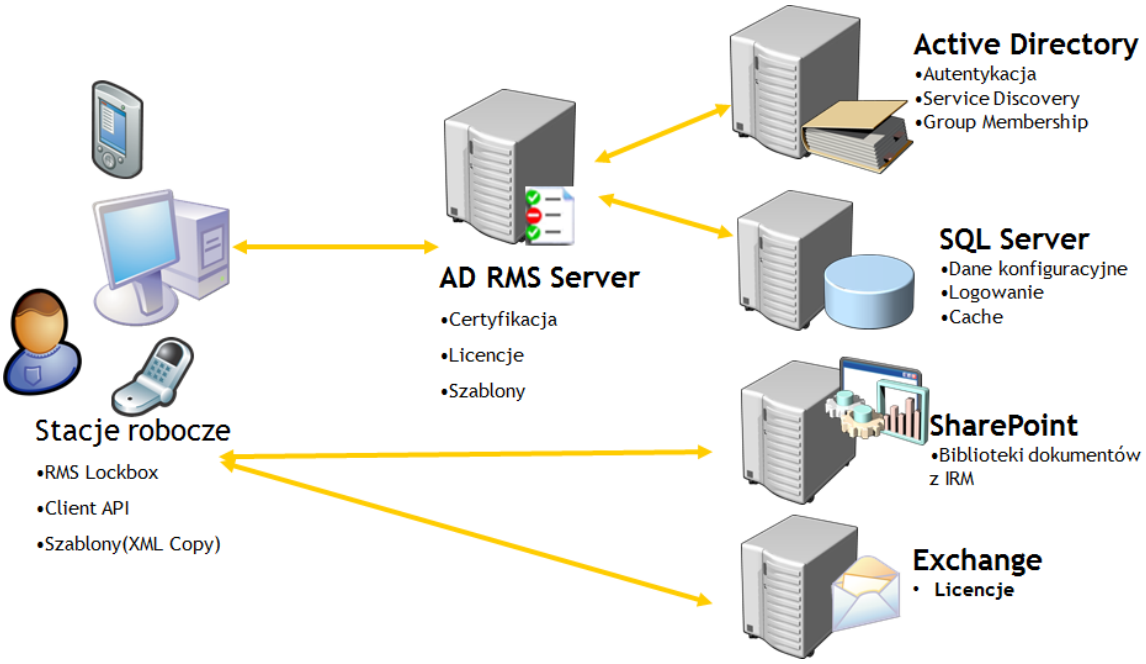
Aby możliwa była praca z IRM koniecznie jest posiadanie usługi Windows Rights Management Services (RMS), uruchomione na platformie Windows Server, oprogramowania Rights Management Update for Windows Client oraz pakietu Office lub innej aplikacji potrafiąca obsługiwać technologię RM. Praca z IRM jest bardzo prosta i nie wymaga większej znajomości technologii przez użytkowników końcowych. Z punktu widzenia administratora systemu wdrożenie takiego rozwiązania to również proces prosty i szybki. Wymaga on jedynie aktywacji serwera RMS, skonfigurowania oprogramowania korzystającego z tych usług oraz aktywacji i rejestracji użytkowników.

Działanie RMS przedstawia się następująco:



Czyli autor informacji za pomocą usługi RMS nakłada reguły na dokumenty, maile i inne informacje oraz pokazuje w jaki sposób można je udostępnić dalej. Sercem rozwiązania jest serwer RMS, który nakłada uprawnienia na informacje i je udostępnia w odpowiedni sposób dla użytkowników.

Komponenty RMS



Warto zwrócić uwagę, że RMS występuje w wersji on-premis jak i online. W tabeli poniżej pokazane jest zestawienie z jakimi aplikacjami poszczególne komponenty współpracują.

App	SharePoint 2013	SharePoint Online 2013	RMS Server	RMS Online
Word, PowerPoint, Excel 2013 (windows)	Tak	Tak	Tak	Tak
Word, PowerPoint, Excel 2013 RT	Tak	Tak	Tak	Tak
Word, PowerPoint, Excel 2010	Tak	Tak (po instalacji Office 365 sign-on assistant.)	Tak	Tak
Office for Mac 2010	Tak	Nie	Tak	Nie
Outlook on Windows Phone 7	Nie dotyczy	Nie dotyczy	Tak	Nie
Word on Windows Phone 7	Tak	Nie	Tak	Nie
Foxit PDF reader on Windows	Tak	Tak (po instalacji Office 365 sign-on assistant.)	Tak	Tak

Exchange

Exchange Server to rozbudowany serwer pocztowy pozwalający na zaawansowaną pracę zarówno od strony użytkownika jak również od strony administratora. Zestaw wbudowanych narzędzi i funkcji pozwala na zapewnienie pełnego bezpieczeństwa danych oraz konfiguracji. Wśród najważniejszych elementów bezpieczeństwa wyróżnić można między innymi:

Ciągła dostępność – system Microsoft Exchange Server 2013 zapewnia kompletne rozwiązanie, jeśli chodzi o wysoką dostępność i przywracanie sprawności systemu po awarii. Tym samym pozwala osiągnąć nowe standardy niezawodności, zapewniające ciągłość działania. Inwestycja w system sprawi, że:

- Wdrażanie złożonych i kosztownych rozwiązań klastrowych stanie się całkowicie zbędne
- Automatyczna replikacja baz danych skrzynek poczty elektronicznej i działanie trybu awaryjnego staną się możliwe przy użyciu zaledwie dwóch serwerów lub pomiędzy rozproszonymi geograficznie centrami obsługi danych
- Możliwa będzie ciągła dostępność systemu i jego szybkie przywracanie dzięki 16 kopiom baz danych poszczególnych skrzynek poczty elektronicznej zarządzanymi przez Microsoft Exchange Server 2013
- Ograniczone zostaną zakłócenia działalności użytkowników podczas przenoszenia skrzynek poczty elektronicznej, co pozwoli na przeprowadzenie zadań migracyjnych oraz konserwacyjnych zgodnie z planem
- Wiadomości email przestaną ginąć z powodu aktualizacji lub awarii serwera transportowego dzięki nowym, wbudowanym funkcjom redundancji zaprojektowanym tak, aby w inteligentny sposób przekierowywać wiadomości inną dostępną drogą.

Archiwizacja i przechowywanie – system Microsoft Exchange Server 2013 oferuje nową wbudowaną funkcję archiwizacji wiadomości email, która pomaga w rozwiązaniu problemów związanych ze zgodnością i ujawnianiem informacji. Nowe usługi pozwalają na:

- Przenoszenie nieporęcznych plików danych programu Outlook (PST) z komputera osobistego na serwer Exchange w celu zapewnienia sprawnej kontroli i ujawnienia w celach prawnych
- Uproszczenie klasyfikacji wiadomości email dzięki nowym regułom przechowywania, które można zastosować do pojedynczych wiadomości lub całych folderów
- Wyszukiwanie we wszystkich skrzynkach pocztowych przy użyciu prostego w obsłudze interfejsu sieci Web lub zlecanie upoważnionym do tego specjalistom ds. kadrowych lub prawnych lub ds. zgodności

Ochrona i kontrola danych - system Microsoft Exchange Server obsługuję funkcję Ochrona i Kontrola Informacji, która upraszcza szyfrowanie, moderowanie i blokowanie wiadomości email o poufnej lub nieodpowiedniej treści na podstawie danych nadawcy, odbiorcy i słów kluczowych. Funkcja ta:

- Łączy system Microsoft Exchange Server z Active Directory Rights Management Services (AD RMS), pozwalając na automatyczne zastosowanie usługi Information Rights Management do informacji w celu ograniczenia wykorzystania danych zawartych w wiadomości i dostępu do nich
- Pozwala partnerom i klientom odczytywać i odpowiadać na wiadomości chronione przez funkcję IRM, nawet, jeżeli nie posiadają oni usługi AD RMS
- Umożliwia kierownikom przeglądanie wiadomości oraz zezwala na ich przekazywanie lub blokowanie

Dokument przedstawia zalecenia dla bezpieczeństwa systemu Exchange wraz z informacjami na temat ich konfiguracji i sposobu użycia. Przed przystąpieniem do instalacji Serwera Microsoft Exchange Server 2013 (każdej z instalowanych w naszym przypadku ról) należy:

- Mieć przygotowaną platformę systemową w postaci serwera Windows Server 2012 Standard Edition w postaci maszyn wirtualnych lub instalacji klasycznej.
- Posiadać zarejestrowaną i skonfigurowaną domenę zewnętrzna DNS, poprawnie skonfigurowane środowisko wewnętrzne DNS Active Directory
- Wykonać aktualizację systemu Windows Server 2012 o najnowsze aktualizacje Windows Update.
- Warto skonfigurować również System Center, dzięki czemu mamy możliwość realizacji wymagania rozporządzenia KRI w zakresie monitorowania, zarządzania i niezaprzeczalności
- Przygotować płytę instalacyjną z Serwerem Microsoft Exchange Server 2013.
- Mieć konto domenowe z uprawnieniami: Domain Administrator , Enterprise Administrator.
- Przed przystąpieniem do instalacji serwera należy zsynchronizować zegar systemowy serwera z kontrolerem domeny:

Aby wykonać takie zadanie trzeba posiadać uprawnienia administracyjne na serwerze. Uruchomić program CMD.EXE jako Administrator. W linii poleceń wpisać komendę „**net time /set /y**".

Antyspam oraz Antymalware

Spam i wirusy były zmorą administratorów system pocztowych w zasadzie od momentu uruchomienia pierwszej usługi pocztowej. W dowolnym momencie każdego dnia ilość wysyłanych maili stanowiących popularny spam rośnie dramatycznie. Exchange Server już od wersji 2003 posiadał wbudowane pewne mechanizmy ochrony przed niechcianą pocztą i wirusami zawartymi w poczcie elektronicznej.

Po konsolidacji ról w serwerze Exchange 2013 agenci anty-spamowi mogą są instalowani na serwerach Client Access Server (CAS), które to dostarczają usługi Front End Transport, która to jest pierwszym punktem kontaktu przychodzących wiadomości email do organizacji.

Wśród agentów anty-spamowych zaliczyć można następujących (działających na serwerach Mailbox):

Sender Filter agent – system analizuje nagłówek pod kątem adresu email nadawcy (MAIL FROM) i porównuje go z domenami, które zostały ustawione przez administratora jako zabronione.

Recipient Filter agent – analizuje wiadomość pod kątem adresu email odbiorcy (RCPT TO) i porównuje go z adresami zdefiniowanymi przez administratora jako zablokowane. Filtr ten również porównuje odbiorców wewnątrz organizacji.

Sender ID agent – zależy od adresu IP wysyłającego serwera oraz Purported Responsible Address (PRA) nadawcy - odpowiada za weryfikację zgodności adresu e-mail z adresem IP nadawcy.

Content Filter agent – analizuje zawartość wiadomości pod kątem występowania określonych treści. Wśród funkcjonalności tego filtru znajduje się między innymi mechanizm kwarantanny, dzięki któremu możemy zmniejszyć ryzyko utraty prawidłowych maili, które z jakiś powodów zostały oznaczone jako spam. Dodatkowo istniej funkcjonalność agregacji bezpiecznych danych (safelist aggregation). Lista ta zbiera dane z Microsoft Outlook oraz Outlook Web App i uzupełnia informację o tym jak użytkownicy klasyfikują pocztę a następnie używa tego przy filtrowaniu.

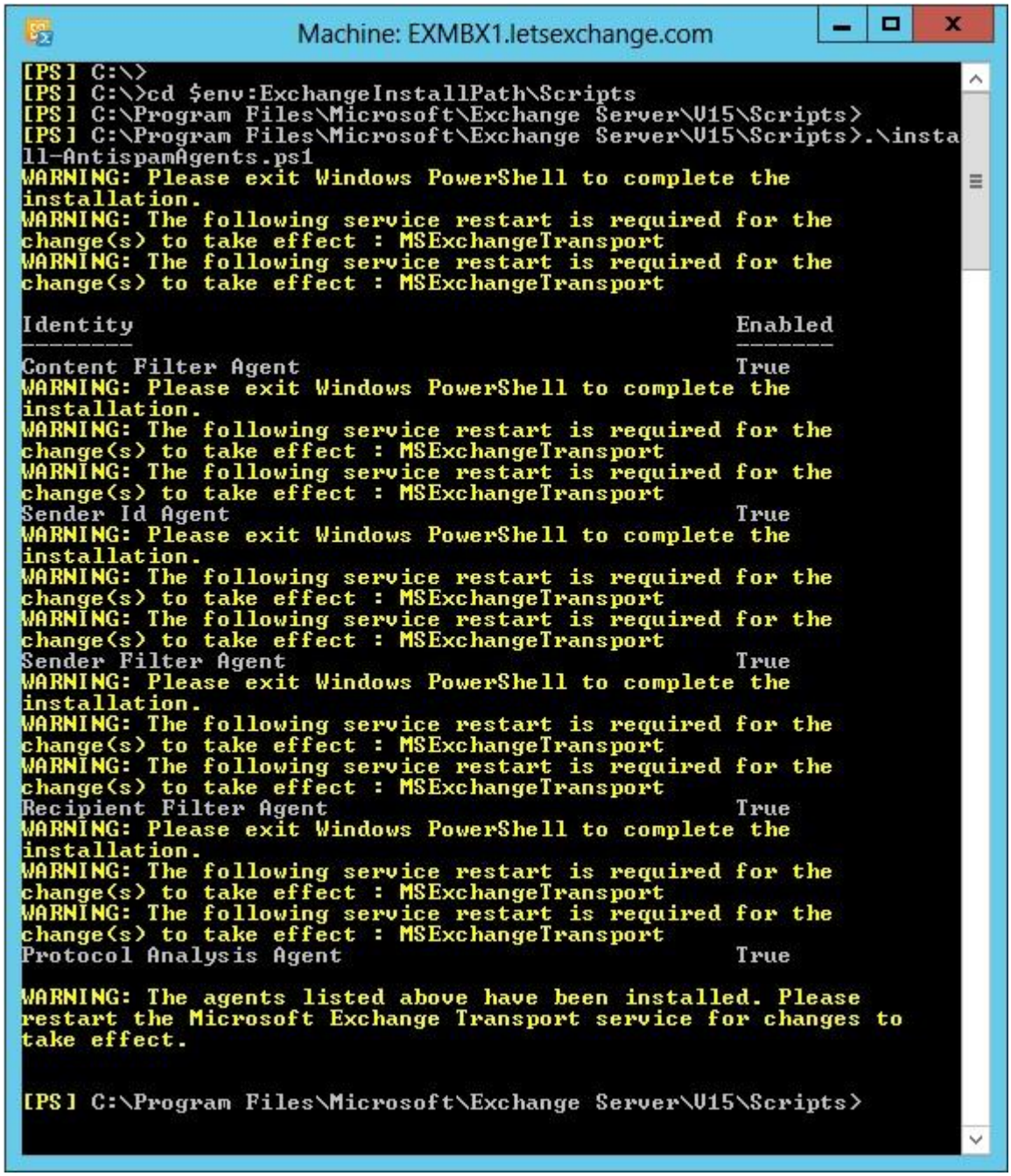
Wśród agentów działających na serwerach Transport zaliczyć można:

Connection Filtering agent – analizuje adresy IP serwera zdalnego, który próbuje wysłać wiadomości aby określić jaką akcję, jeśli w ogóle, należy podjąć z przychodzącą wiadomością. Filtrowanie połączeń używa różnych list zablokowanych i nieblokowanych adresów IP.

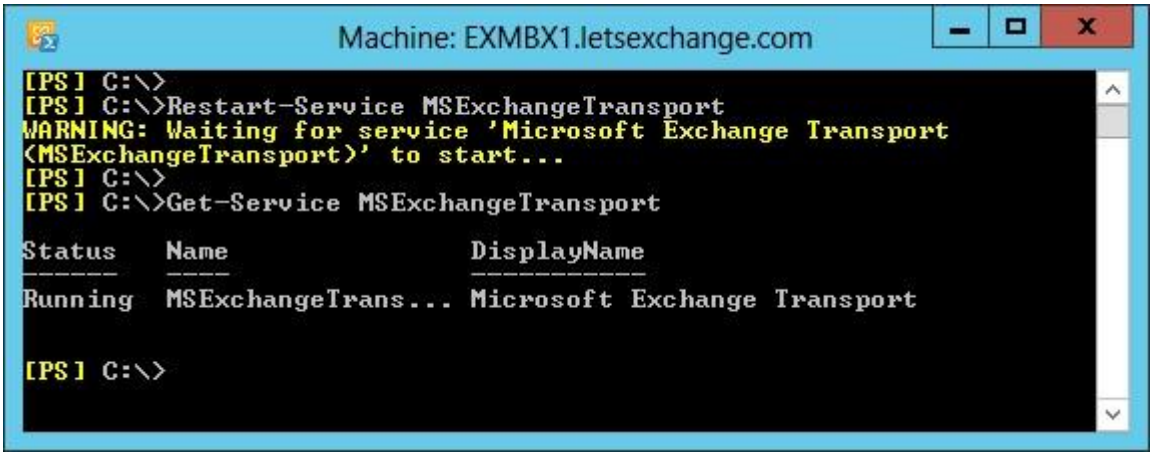
Attachment Filter agent – filtruje wiadomości bazując na nazwie pliku, rozszerzeniu oraz typu zawartości MIME. Filtr ten można skonfigurować w taki sposób, że załącznik z widomości będzie kasowany a wiadomość przesłana dalej lub kasować całą wiadomość wraz z załącznikiem.

Aby uruchomić funkcje antyspamowe należy wykonać skrypt PowerShell:

Install-AntispamAgents.ps1



Następnie należy wykonać restart usługi transportowej



Ostatnim krokiem jest określenie wszystkich adresów IP wewnętrznych serwerów SMTP, które powinny być ignorowane przez SenderID – musi być podany przynajmniej jeden adres IP.

Podobnie wygląda sytuacja z wbudowanym silnikiem Anti-malware w Exchange 2013. Jest to element produktu Forefront Protection for Exchange 2010. Podczas instalacji instalator domyślnie podpowiada opcję włączenia silnika, o ile firma nie używa innego produktu antywirusowego.

Włączenie tej opcji możliwe jest również za pomocą skryptu PowerShell, który znajduje się w folderze Scripts katalogu instalacyjnego Exchange 2013:

Enable-antimalwareScanning.ps1

A następnie wykonać restart usługi Transport

Zarządzanie dostępem mobilnym

Jednym z aspektów bezpieczeństwa może być określenie czy możliwy jest dostęp mobilny dla danego konta i ewentualnie, z jakiego typu urządzeń - jeśli tak.

Aby dostęp mobilny był możliwy w organizacji Exchange należy posiadać poprawnie skonfigurowany serwer DNS (zewnętrzny i wewnętrzny). Posiadać należy również certyfikat, który będzie wystawiony przez zaufany główny urząd certyfikacji (Np. Certum, Verisign, Geotrust itp.) dla domeny, pod którą będzie widoczny serwer dostępowy Exchange (Client Access Server).

Istotną kwestią jest fakt, iż w systemach typu Windows Phone klucz publiczny głównego urzędu certyfikacji, który wydał certyfikat dla domeny z exchange, musi być dograny do systemu operacyjnego Windows Phone. Może, bowiem zdarzyć się, iż certyfikat nie będzie zainstalowany wówczas synchronizacja urządzenia z serwerem Exchange nie będzie możliwa.

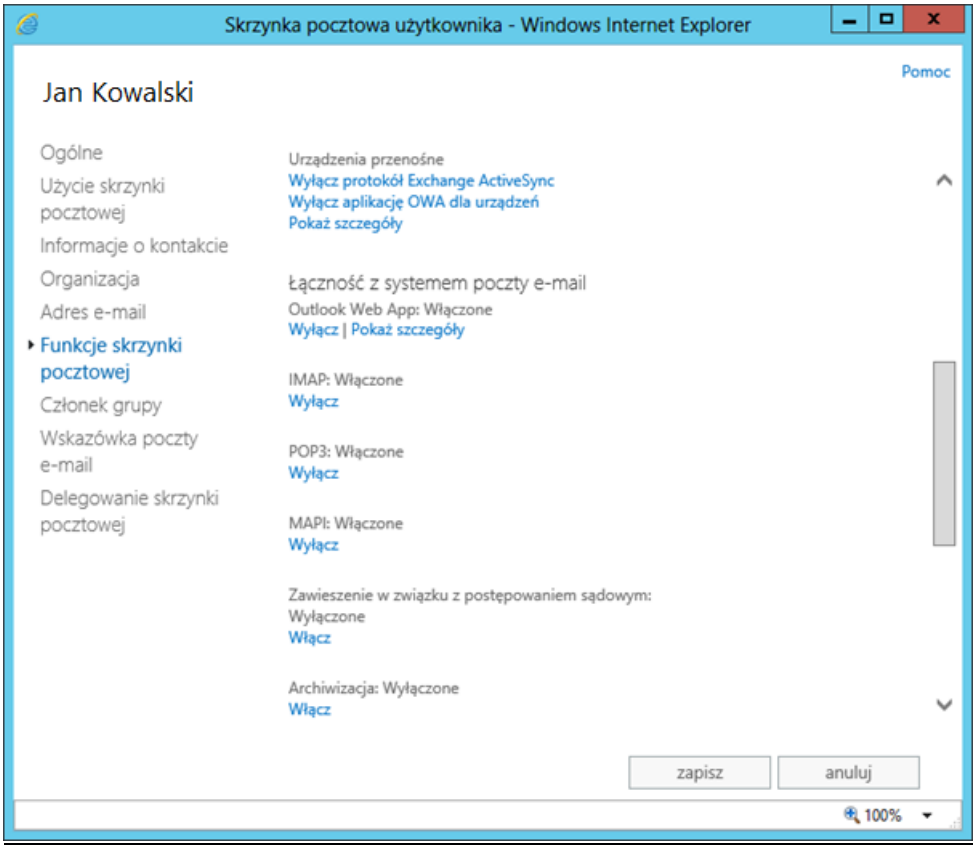
Przydzielenie/Odebranie dostępu mobilnego.

Z założenia przy tworzeniu nowego konta exchange dostęp do usług POP3/IMAP4/Activesync (Dostęp mobilny) jest włączony.

Aby nadać możliwość dostępu mobilnego do skrzynki pocztowej należy zalogować się do konsoli zarządzania Exchange wykorzystując link: *Https://ex-cas01/ecp*

Przechodzimy do zakładki *Adresaci → Skrzynki Pocztowe*. Wybieramy konto, dla którego chcemy zmodyfikować uprawnienie dostępu mobilnego.

Przechodzimy do zakładki *Funkcje skrzynki pocztowej* (patrz rysunek poniżej)



Modyfikujemy opcję Urządzenia Przenośne. Ustawiamy Wyłącz protokół Exchange ActiveSync.

Jeśli chcemy taki dostęp włączyć wówczas postępujemy identycznie z tym, że wybieramy *Włącz protokół Exchange ActiveSync.*

Aby wykonać operację wyłączenia dostępu ActiveSync dla wszystkich kont w Organizacji Exchange należy zalogować się do Exchange Management Shell i wykonać poniższe polecenie:

Get-CASMailbox|Set-CASMailbox -ActiveSyncEnabled $false

Jeśli chcemy włączyć dostęp mobilny dla użytkowników Exchange należy wykonać polecenie:

Get-CASMailbox|Set-CASMailbox -ActiveSyncEnabled $true

Określanie parametrów dostępu.

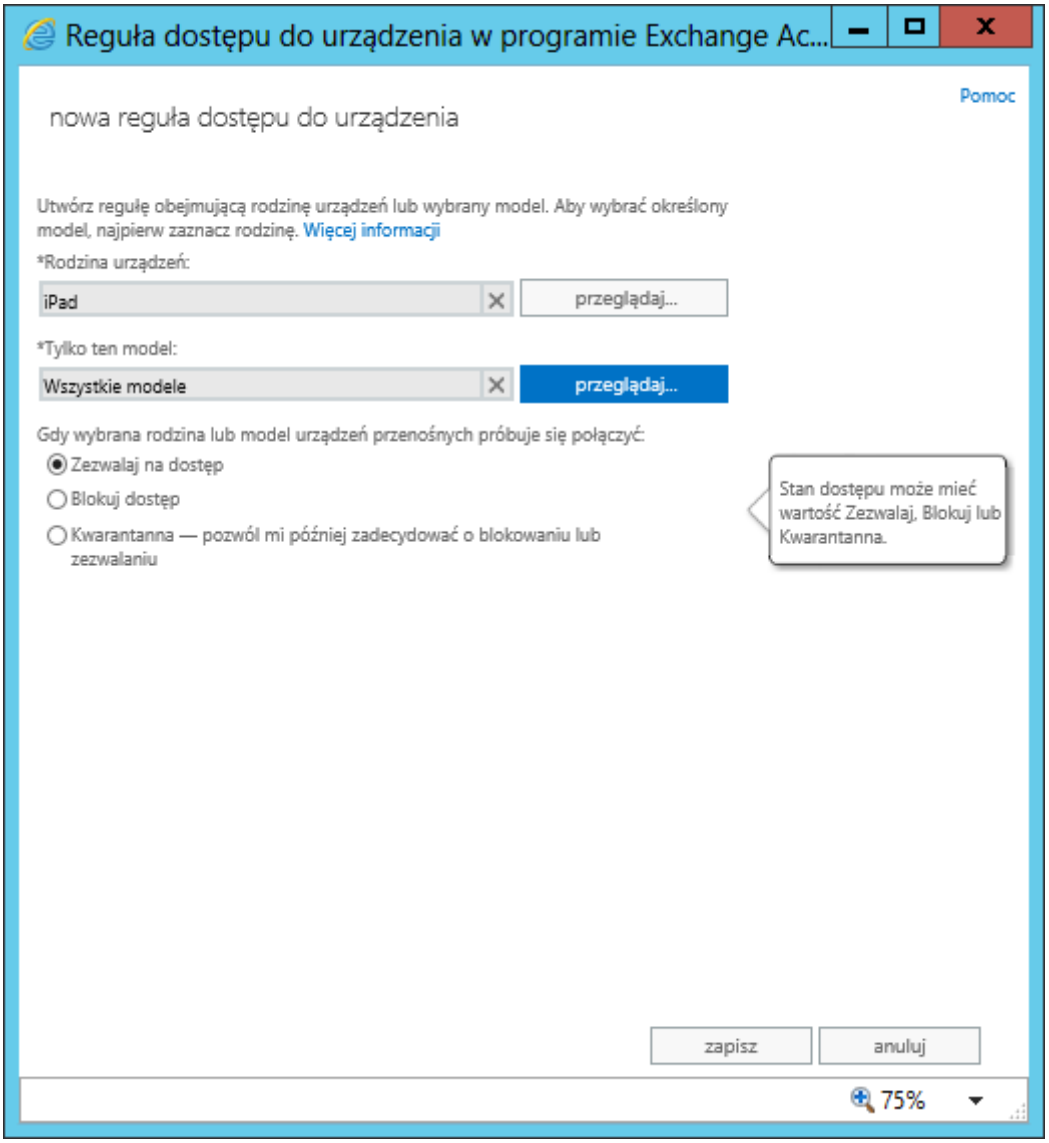
Określanie zasad dostępu ActiveSync odbywa się za pomocą polityk.

Aby utworzyć politykę dostępu ActiveSync należy zalogować się do konsoli zarządzania Exchange wykorzystując link: *Https://ex-cas01/ecp*

Przechodzimy do zakładki Mobilne → Dostęp z urządzenia mobilnego. W pozycji Reguły dostępu do urządzeń wybieramy 

Zakładka ta daje nam możliwość zdefiniowania różnych polityk dla różnych typów urządzeń (np. iOS, Windows Phone, Android)

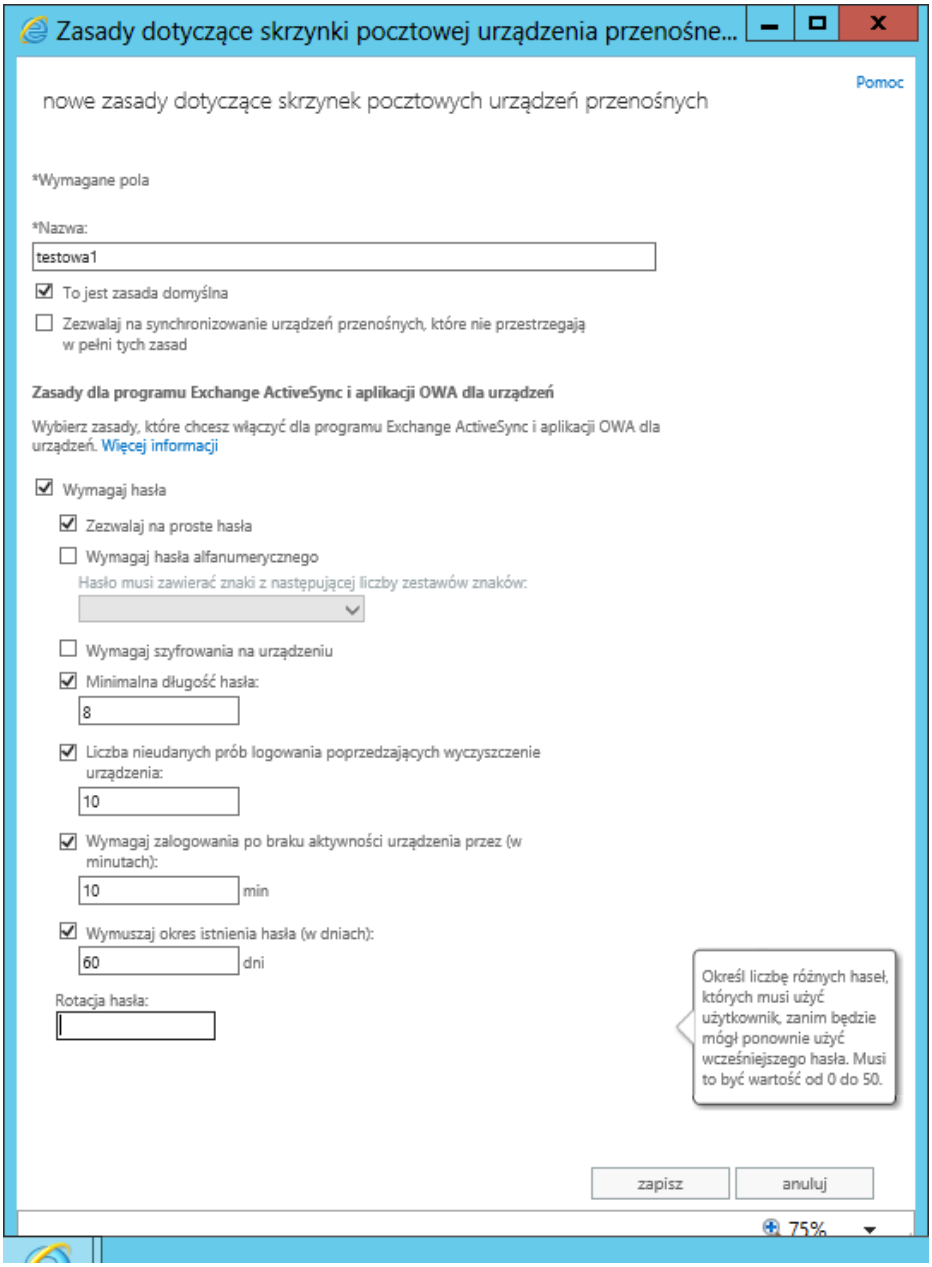
Patrz rysunek poniżej.



Następnym krokiem jest utworzenie nowej zasady skrzynek pocztowych dla urządzeń przenośnych.

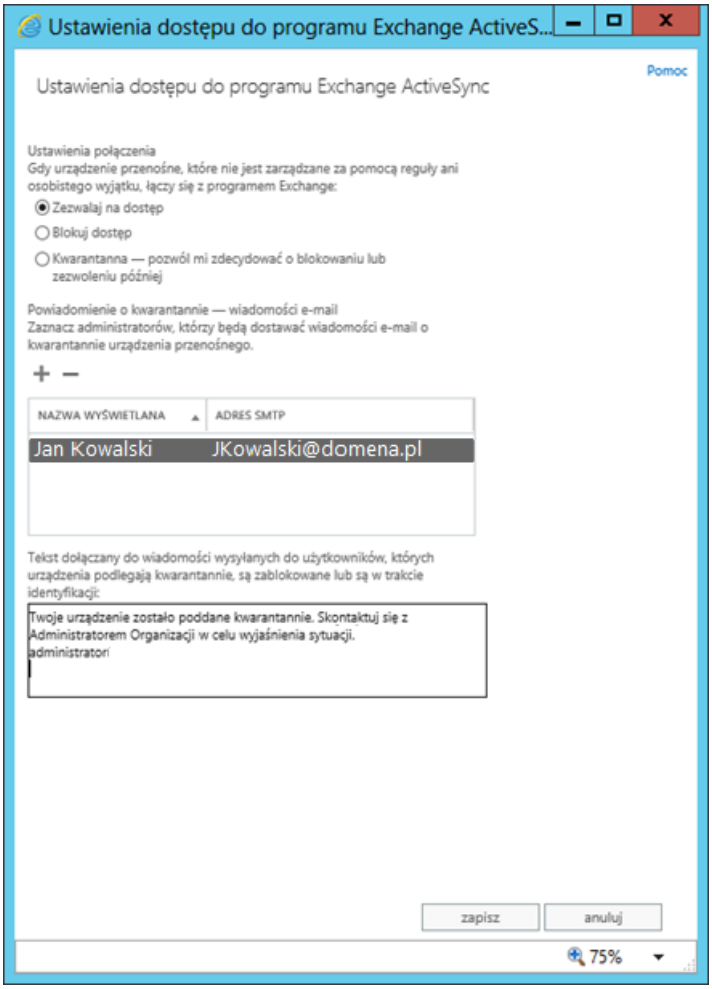
Aby to wykonać należy przejść do zakładki Zasady skrzynek pocztowych dla urządzeń przenośnych

Wybieramy + i definiujemy nową politykę. Ustawiając parametry zgodnie z własnym żądaniem. (patrz rysunek poniżej).



Opcje Administracyjne dostępu mobilnego

Aby zdefiniować opcje administracyjne dostępu mobilnego należy przejść do zakładki *Dostęp z urządzenia mobilnego* i wybrać *Edytuj* (patrz rysunek poniżej)



Opcje te pozwalają na określenie, kto ma otrzymywać informację, jeśli urządzenia zostaną poddane kwarantannie jak również określenie tekstu, jaki ma się pojawić w wiadomości wysłanych do użytkowników, których urządzenia mobilne podlegają kwarantannie.

Reguły

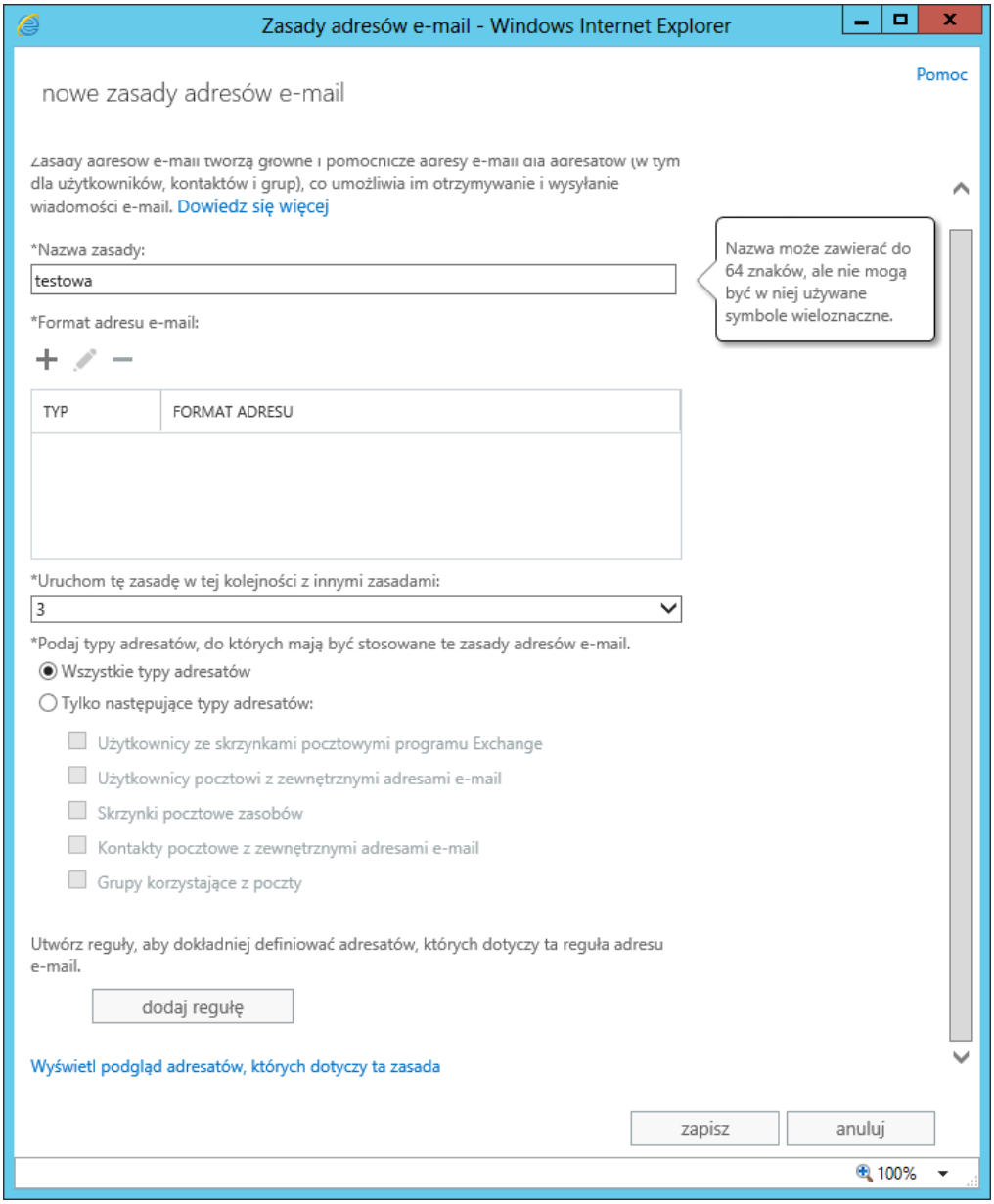
Zarządzanie politykami mailowymi organizacji Exchange daje możliwość ustawiania konwencji nazewniczej oraz nazw domen, jakie mają być przypisywane użytkownikom organizacji Exchange.

Można to wykonać z poziomu konsoli zarządzania Exchange logując się wykorzystując link:

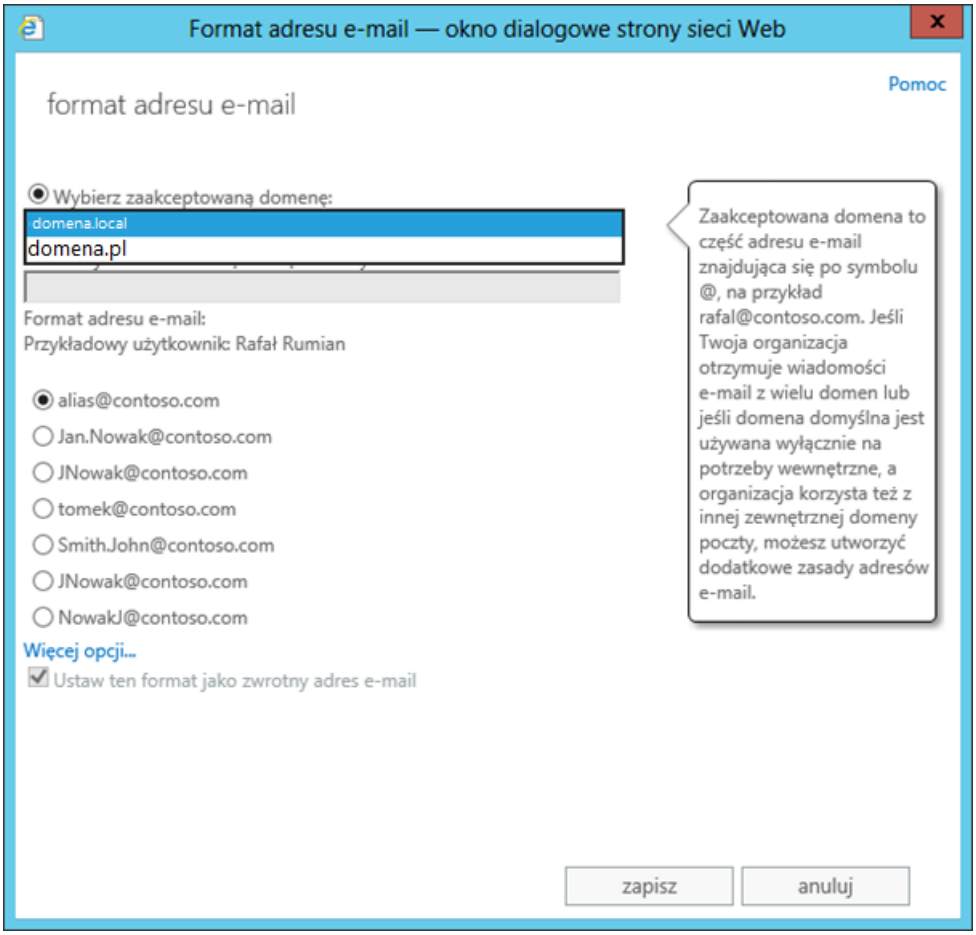
Https://ex-cas01/ecp

Następnie przechodząc do zakładki *Przepływ poczty → Zasady adresów E-mail*

Klikamy pozycję + .Otworzy nam się nowe okno pozwalające na utworzenie nowej polityki adresowej (patrz rysunek poniżej na następnej stronie). Definiujemy nazwę tej polityki,



klikamy na  aby utworzyć format adresu e-mail (patrz rysunek poniżej na następnej stronie)



*Należy pamiętać, że aby utworzyć nową politykę adresową musimy mieć już dodaną domenę akceptowalną w organizacji Exchange.

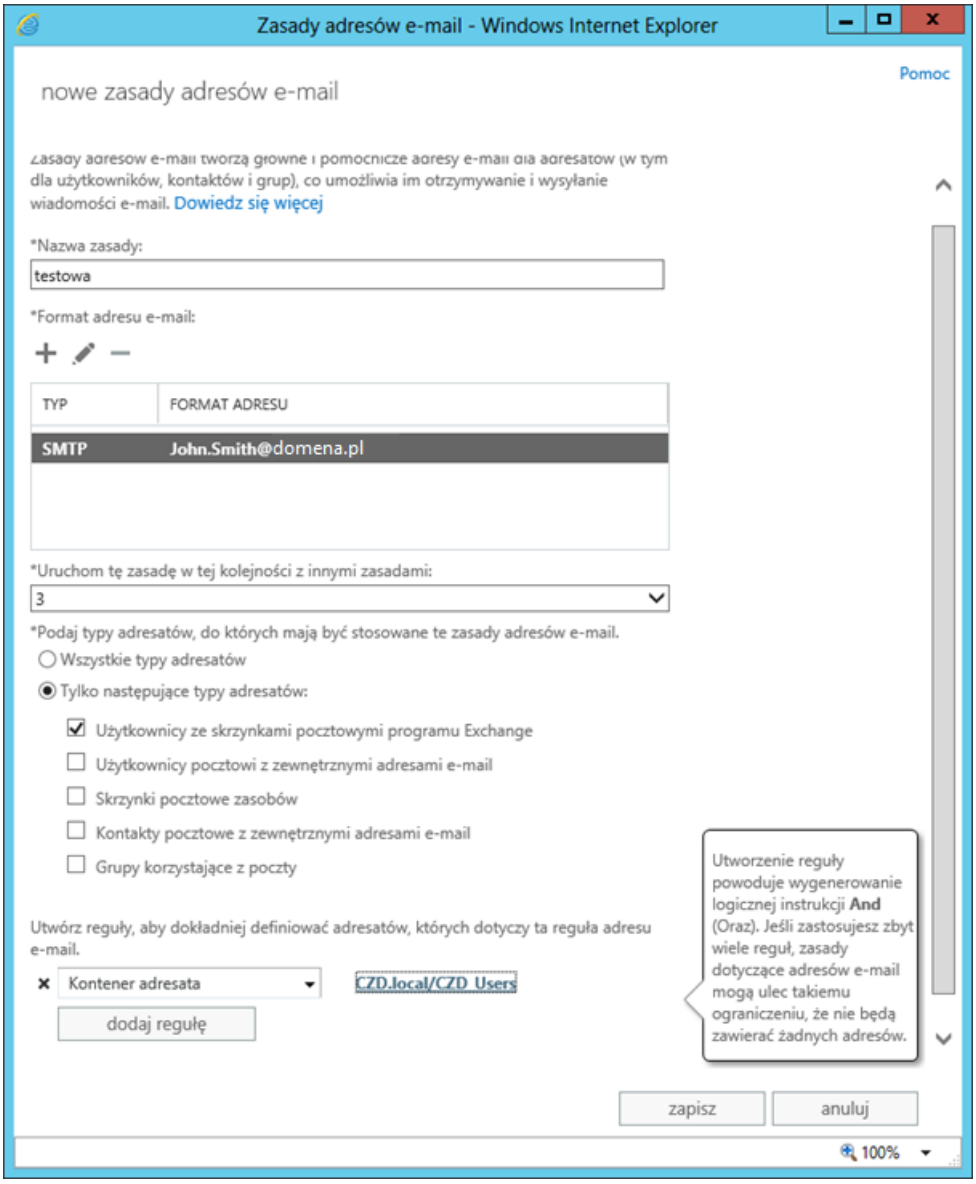
Definiujemy format adresu e-mail i klikamy *Zapisz*.

Deklarujemy opcje dla pola Uruchom tę zasadę w tej kolejności z innymi zasadami.

**istotna rzecz to priorytet; im niższa cyfra tym wyższy priorytet. Należy pamiętać, że tylko jedna zasada może działać w danym momencie.*

Następnym krokiem jest zdefiniowanie, do kogo ma być przypięta polityka (Jakich użytkowników ma dotyczyć). Wybieramy odpowiednią opcje w polu *Podaj typy adresatów, do których mają być stosowane… (patrz rysunek poniżej na następnej stronie)*

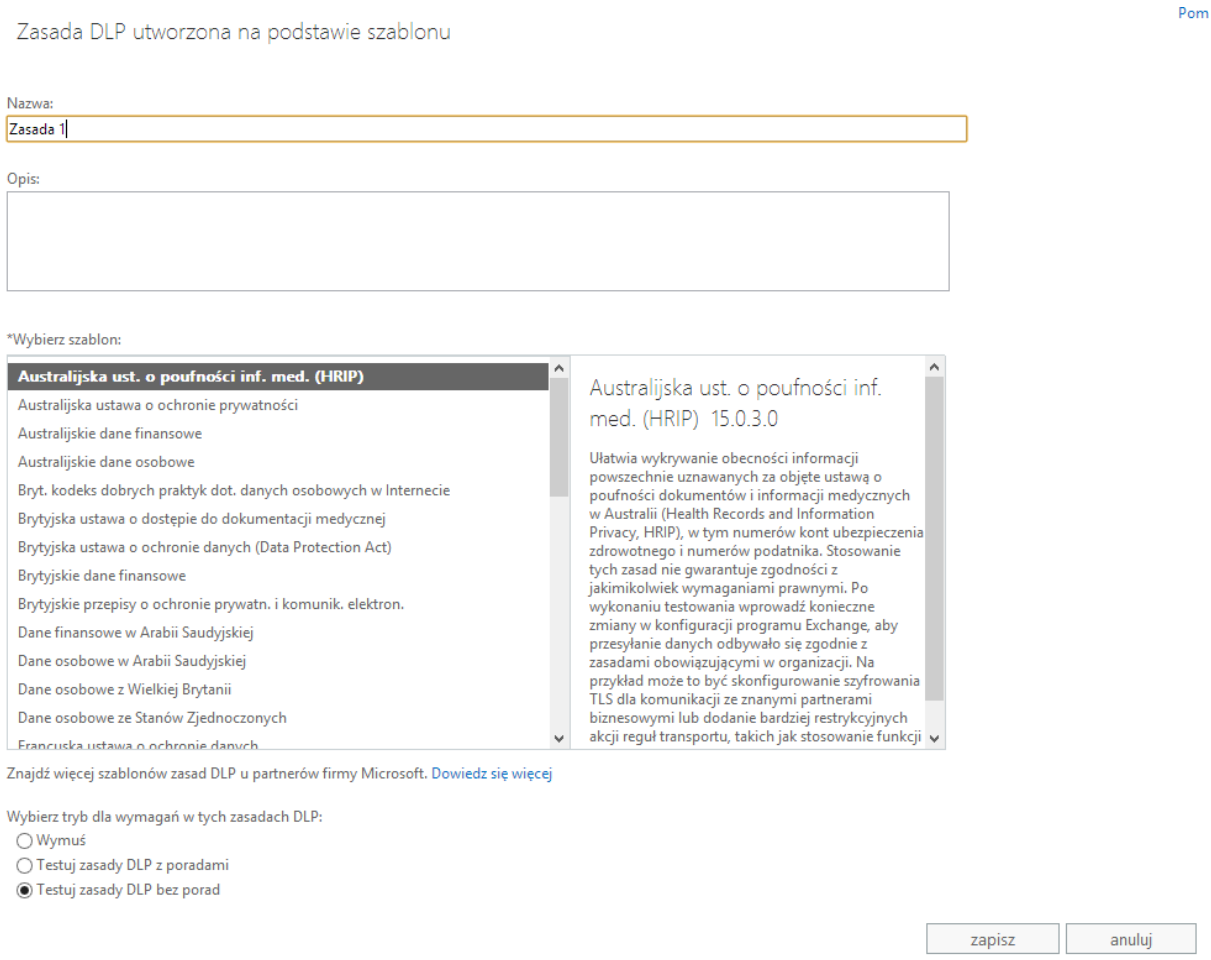
Można wykonać również większą filtrację użytkowników, których obowiązywać polityka. W tym celu należy utworzyć regułę, określającą których użytkowników ma dotyczyć polityka. Pole *Utwórz reguły, aby dokładniej definiować adresatów…*



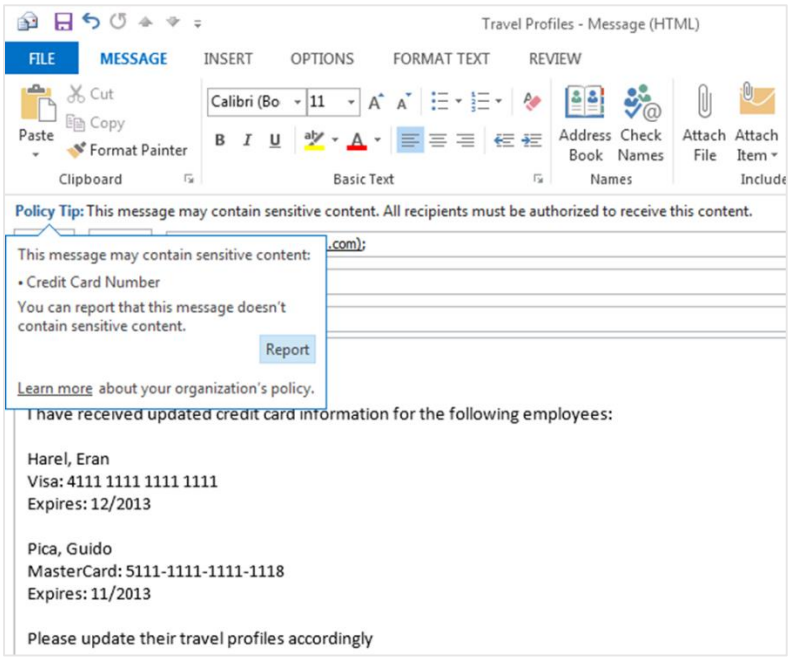
Data Loss Prevention - DLP

Częstym problemem związanym z bezpieczeństwem jest utrata poufnych danych, czy to w tekście maila czy jako załącznik. W Exchange Server 2013 wprowadzona została nowa funkcjonalność Data Loss Prevention, która ma za zadanie „pilnowania" przepływu wiadomości w obrębie systemu pocztowego Exchange Server. Dzięki funkcjonalności DLP administrator może zablokować wysyłkę maili, w których znajdują się poufne informacje takie jak numery kart kredytowych czy inne, automatycznie informując o incydencie odpowiednie osoby w firmie.

Konfiguracja zasad wygląda następująco – w opcjach zarządzania zgodnością, wybieramy opcję ochrony przed utratą danych – tam dodajemy kolejne zasady:



Po stworzeniu zasady ochrony Outlook będzie informował użytkownika o złamaniu danej zasady:



Audyty

Exchange Server udostępnia administratorowi zestaw raportów, które pozwalają znaleźć zmiany wprowadzone w skrzynkach pocztowych i ustawieniach konfiguracyjnych. Możliwe jest odnalezienie określonego typu zmian, a następnie wyeksportować wyniki do pliku, który zostanie wysłany do administratora lub innych użytkowników.

Wśród standardowych raportów dostępne są:

Raport o dostępie do skrzynki pocztowej przez osoby niebędące jej właścicielami - Wyszukiwanie dzienników inspekcji skrzynek pocztowych, które były otwierane lub modyfikowane przez osoby inne niż ich właściciele.

Raport o grupie ról administratorów - Wyszukiwanie w dzienniku inspekcji administratora zmiany wprowadzone w grupach ról. Grupy ról służą do przypisywania użytkownikom uprawnień administracyjnych.

Raport o miejscowym zbieraniu i blokadzie elektronicznych materiałów dowodowych - Wyszukiwanie w dzienniku inspekcji administratora zmiany wprowadzone w miejscowym zbieraniu i blokadzie elektronicznych materiałów dowodowych

Raport o zawieszeniach spowodowanych postępowaniem sądowym dla poszczególnych skrzynek pocztowych - Wyszukiwanie w dzienniku inspekcji administratora użytkowników, dla których skrzynek pocztowych włączono lub wyłączono zawieszenie spowodowane postępowaniem sądowym.

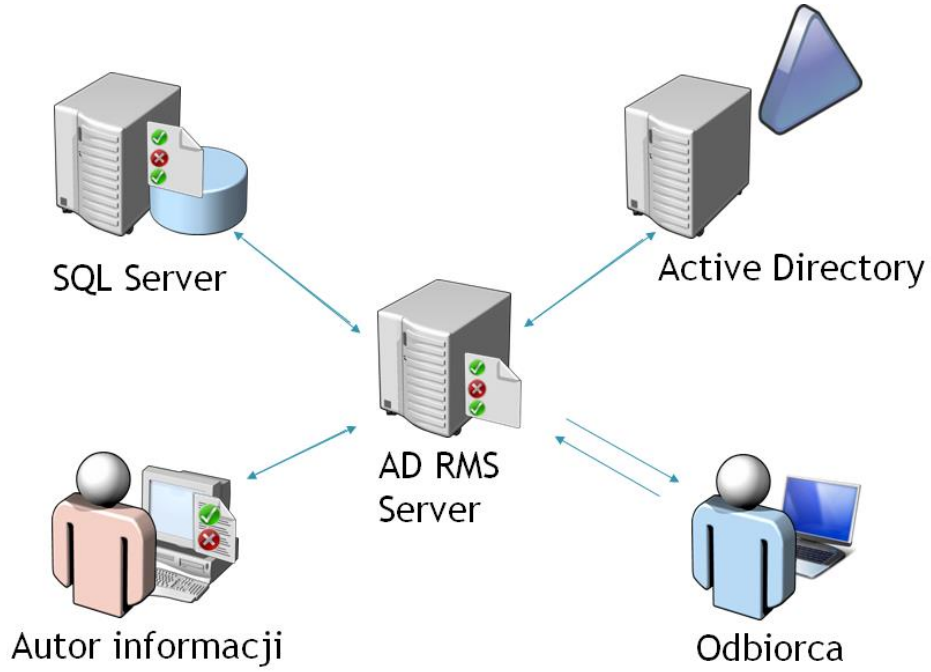
Eksportuj dzienniki inspekcji skrzynek pocztowych - Wyszukiwanie i eksportowanie informacji o dostępie do skrzynki pocztowej przez osoby inne niż właściciel

Eksportuj dziennik inspekcji administratora - Wyszukiwanie i eksportowanie informacje o zmianach konfiguracji wprowadzonych w Twojej organizacji

RMS/IRM

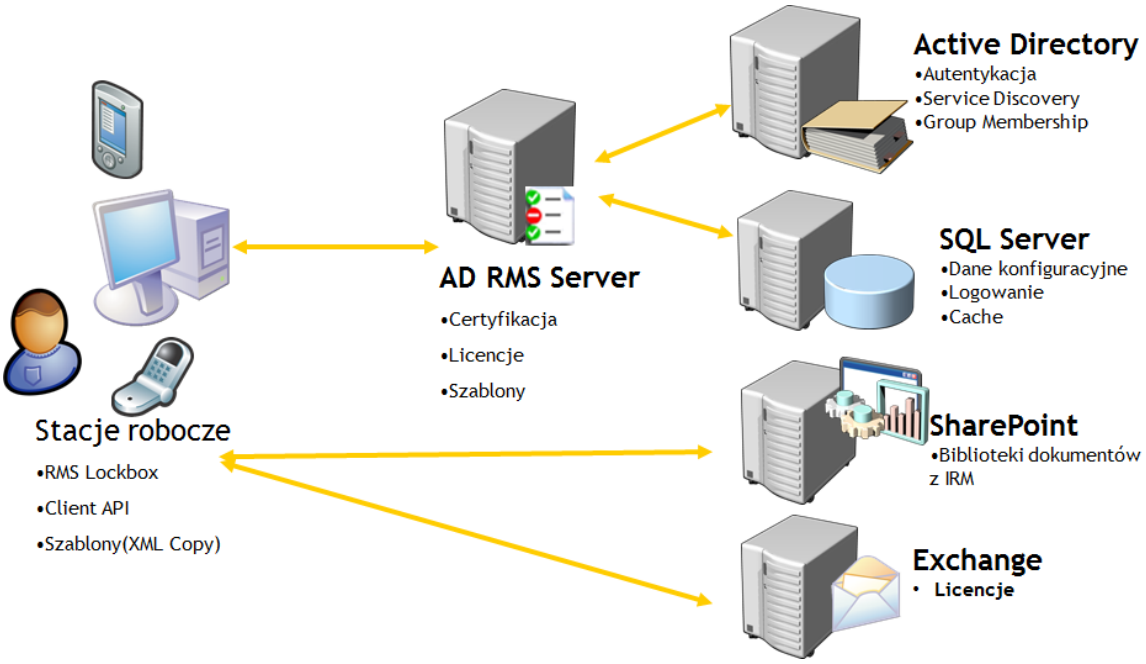
Usługa Active Directory Rights Management Services - za pomocą tej usługi dostępnej w ramach Active Directory możliwe jest zarządzanie prawami dostępu do różnych informacji w firmie, chroniąc informacje za pomocą stałych zasad użytkowania, które są dołączone do informacji niezależnie od tego, dokąd te informacje są przenoszone. Za pomocą usługi AD RMS można zapobiegać zamierzonemu lub przypadkowemu ujawnieniu poufnych informacji, takich jak raporty finansowe, specyfikacje produktów, dane klientów i poufne wiadomości e-mail. Usługa ta idealnie integruje się z Exchange oraz usługami SharePoint Portal Server. W przypadku RMS wymagane jest posiadanie licencji CAL dla użytkowników.

Działanie RMS przedstawia się następująco:



Czyli autor informacji za pomocą usługi RMS nakłada reguły na dokumenty, maile i inne informacje oraz pokazuje w jaki sposób można je udostępnić dalej. Sercem rozwiązania jest serwer RMS, który nakłada uprawnienia na informacje i je udostępnia w odpowiedni sposób dla użytkowników.

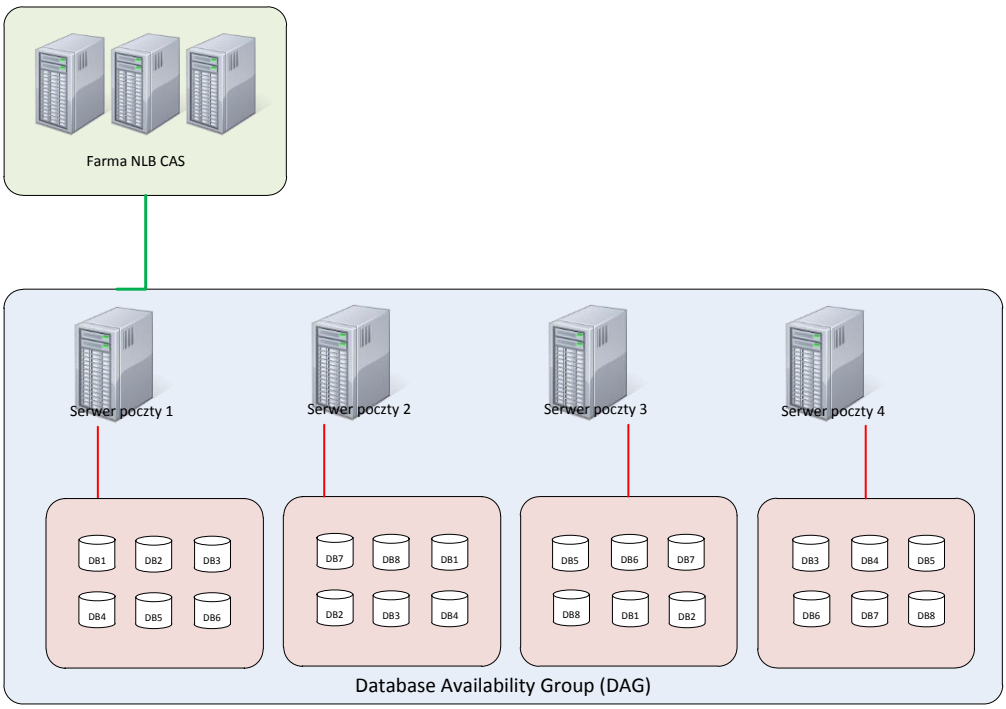
Komponenty RMS



Database Availability Groups (DAG) -bezpieczeństwo utraty danych

Aby zapewnić wysoką dostępność poczty i pełne bezpieczeństwo danych należy rozważyć użycie mechanizmów dostępnych w Exchange - **Database Availability Groups**.

Database Availability Groups jest grupą serwerów, która pozwala zapewnić wysoką dostępność serwerów Mailbox w Organizacji. Pojedynczy serwer Mailbox w zależności od posiadanej wersji Exchange pozwala przechowywać od kilku do kilkunastu baz danych. Exchange Server używa mechanizmu ciągłej replikacji (continuous replication) baz skrzynek pocztowych pomiędzy serwerami należącymi do Database Availability Group w celu zapewnienia aktualnej kopi bazy danych na wszystkich serwerach. Aktywny log transakcyjny aktywnej bazy danych jest zapisywany i zamykany. Następnie usługa Microsoft Exchange Replication replikuje zamknięty log do serwerów utrzymujących pasywną kopię bazy danych. Zreplikowany log jest weryfikowany pod kątem integralności, nagłówek po nagłówku. Następnie usługa Information Store odtwarza dzienniki transakcyjne i synchronizuje pasywne kopie bazy danych. Dzięki temu każda kopia bazy danych jest identyczna i aktualna.



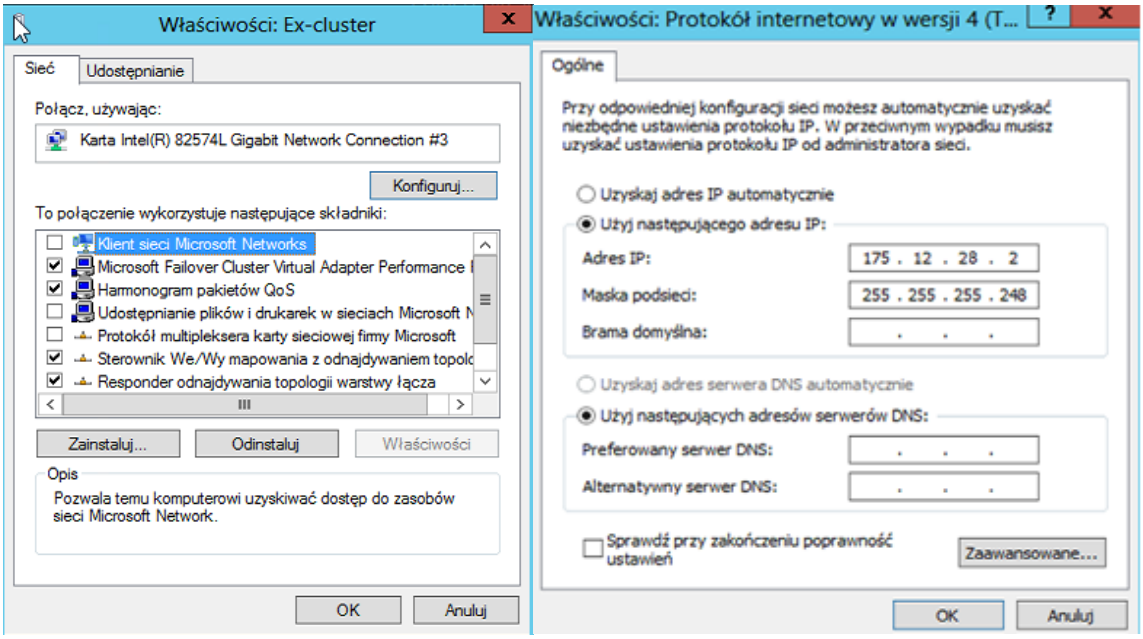
Przed przystąpieniem do konfiguracji DAG należy na każdym serwerze, który ma być członkiem DAG zainstalować component Windows “Failover Cluster Manager” (pol. Menadżer klastra pracy awaryjnej)

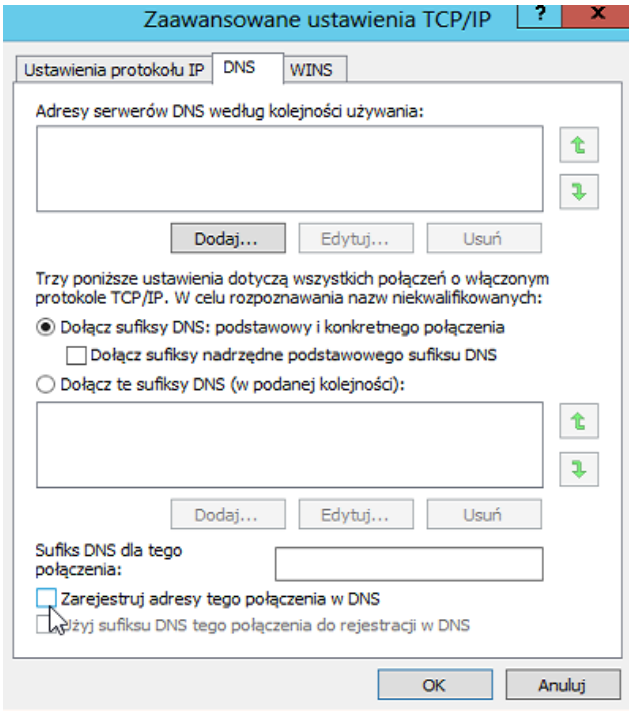
Konfiguracja kart sieciowych

W pierwszej kolejności, aby móc przystąpić do konfiguracji DAG należy mieć przygotowany interface, który będzie służył tylko do komunikacji między członkami DAG. (patrz rysunki poniżej)

Konfiguracja interface’u powinna wyglądać następująco:

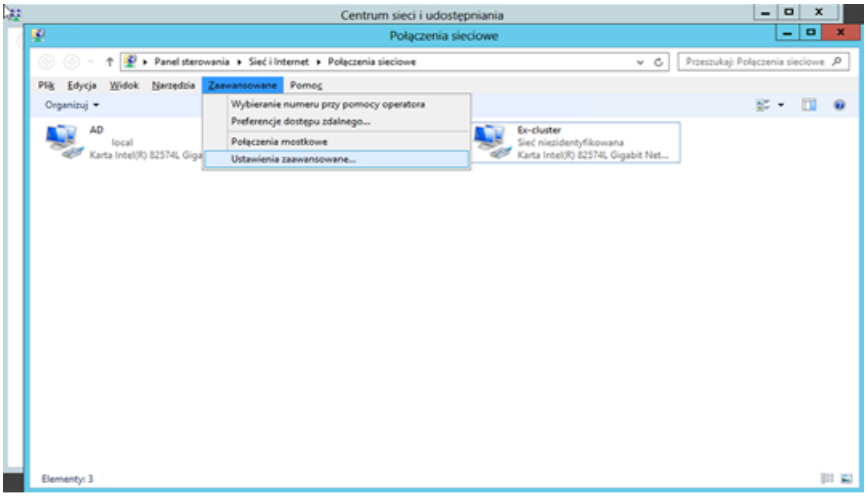
- Brak zdefiniowanego Default Gateway w konfiguracji protokołu TCP/IP
- Nie powinien rejestrować swojej nazwy w serwerze DNS Active Directory.
- Nie powinien mieć włączonych usług: „Klient Sieci Microsoft Networks", „Udostępnianie plików i drukarek..."



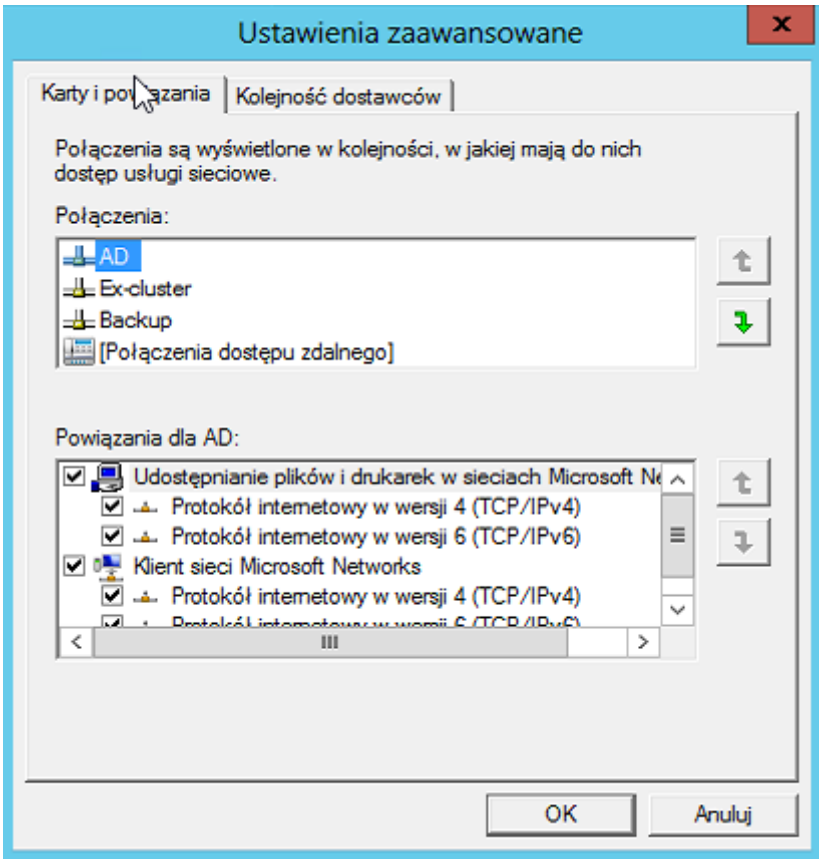


Następnym krokiem jest ustawienie kolejności Podłączania kart sieciowych (BIND)

Aby wykonać tą operację, należy dostać się do zarządzania kartami sieciowymi sytemu Windows (Połączenia sieciowe) wybrać właściwości.



Następnie ustawić kolejność powiązania zgodnie z rysunkiem:



Instalowanie Database Availibility Group.

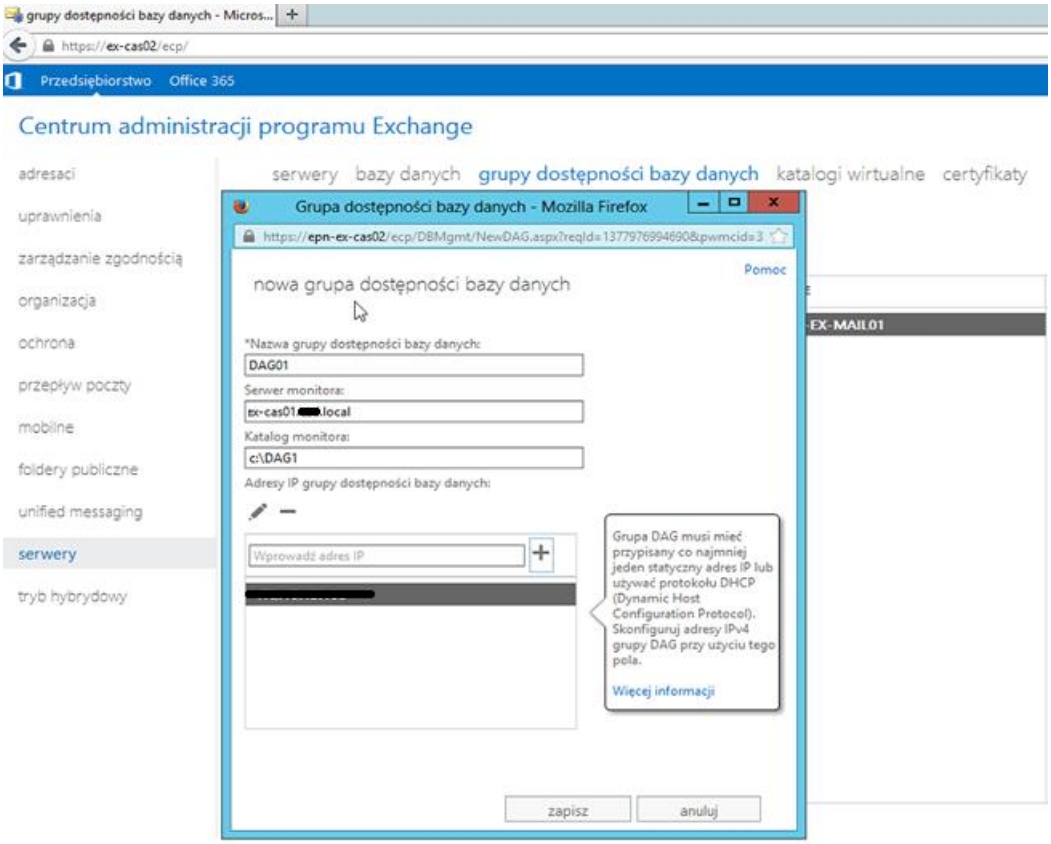
Aby móc skonfigurować grupę DAG należy zalogować się do Konsoli zarządzania Microsoft Exchange używając poniższego linku (Użytkownik musi posiadać uprawnienia Enterprise Admin) – przykładowy link (w naszej konfiguracji system składa się z dwóch maszyn CAS, dwóch maszyn w rolach Mail i Hub oraz serwer w roli Edge)

https://ex-cas01/ecp

Przed przystąpieniem do tworzenia nowego Cluster'a DAG, należy przygotować nowy obiekt typu *Computer* w naszej domenie. Następnie należy to konto wyłączyć (Disable account).

Po wykonaniu tej operacji należy nadać uprawnienia FULL CONTROL dla grupy *Exchange trusted subsystem*

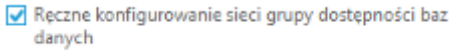
Przejść do grupy Serwery → Grupy Dostępności Bazy Danych i wybrać ikonę + aby dodać nową grupę DAG. Następnie wpisać dane zgodnie z rysunkiem:



Gdzie:

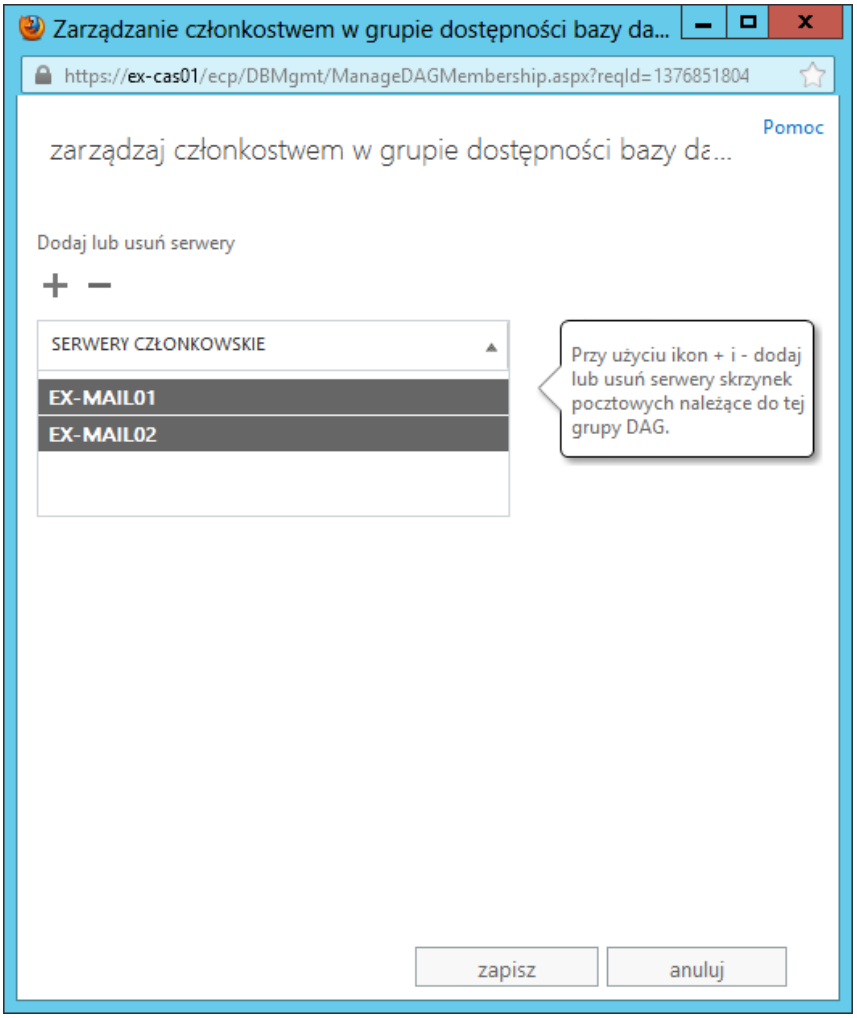
- Nazwa Grupy Dostępności bazy danych to nazwa, pod jaką będzie widoczny klaster w sieci LAN (tworzony jest obiekt typu Komputer)
- Serwer Monitora to serwer Quorum Klastra
- Katalog Monitora (to katalog, w którym trzyma się dane klastrowe)
- Adres IP to adres, pod jakim klaster będzie widoczny w sieci LAN

PO utworzeniu grupy należy wybrać opcje edycji stworzonej uprzednio grupy i w zakładce Ogólne zaznaczyć i nacisnąć zapisz.

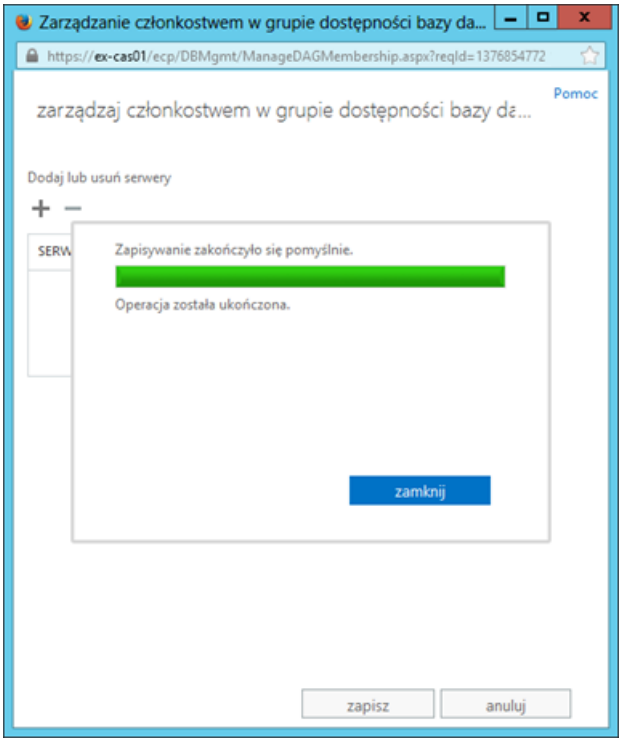


Następnie wybrać „Zarządzaj Członkostwem w grupie DAG”

Wybrać serwery członkowskie w danym klastrze DAG (patrz rysunek) i nacisnąć „Zapisz”



Czas trwania konfiguracji Grupy DAG może być dość długi. Na koniec powinna się pojawić informacja o pomyślnej instalacji i konfiguracji składników grupy DAG – rysunek:



Wyłączenie sieci służącej do Backup'u danych z członkostwa grupy DAG

Przy konfiguracji DAG instalator automatycznie konfiguruje sieci wykorzystywane do sieci DAG. Kryteria takiego wyboru są następujące:

Sieć Dla ruchu MAPI (dla klientów Exchange np. Outlook) posiada następujące kryteria:

- Ustawiony Default Gateway
- Ustawiony serwer DNS
- Włączone rejestrowania nazwy w DNS

Sieć dla ruchu klastra DAG:

- Brak Default Gateway
- Brak wpisanego serwera DNS
- Brak rejestracji nazwy w DNS

Aby usunąć sieć należy w Konsoli Management Shell wykonać poniższą komendę:

Set-DatabaseAvailabilityGroupNetwork -Identity dag01\replicationdagnetwork02 -ReplicationEnabled:$false -IgnoreNetwork:$true

Gdzie Dag01\replicationdagnetwork02 to sieć do Backup 'u danych

Aby sprawdzić skuteczność wykonania komendy należy wpisać:

Get-DatabaseAvailabilityGroupNetwork

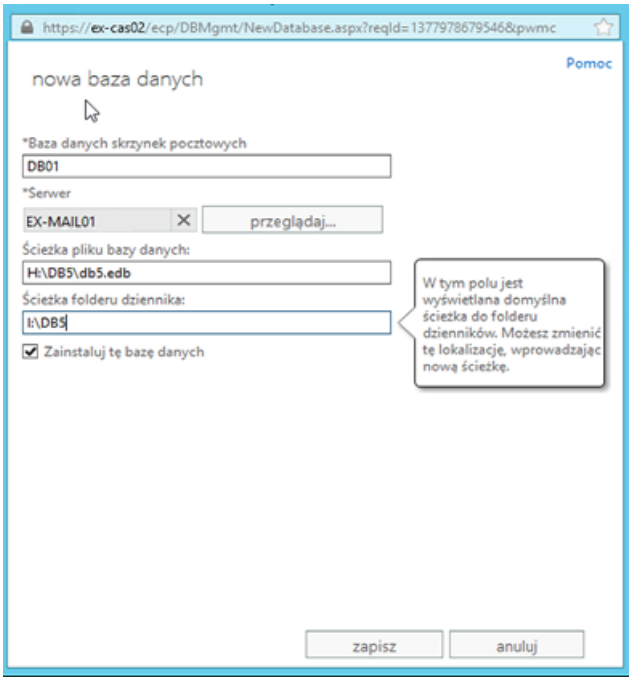
Identity	ReplicationEnabled	Subnets
DAG01\MapiDagNetwork	True	{{175.26.13.109/29, Up}}
DAG01\ReplicationDagNetwork01	True	{{175.26.21.0/29, Up}}
DAG01\ReplicationDagNetwork02	**False**	{{175.26.18.0/24, Up}}

Dodawanie Baz Danych

Aby móc dodać bazy danych do konfiguracji serwera Microsoft Exchange Server 2013 należy zalogować się do konsoli zarządzania Exchange używając poniższego linku:

Https://ex-cas01/ecp

Następnie przejść do „Serwery" → „Bazy Danych" i wybrać ikonę + i postępować zgodnie z rysunkiem:

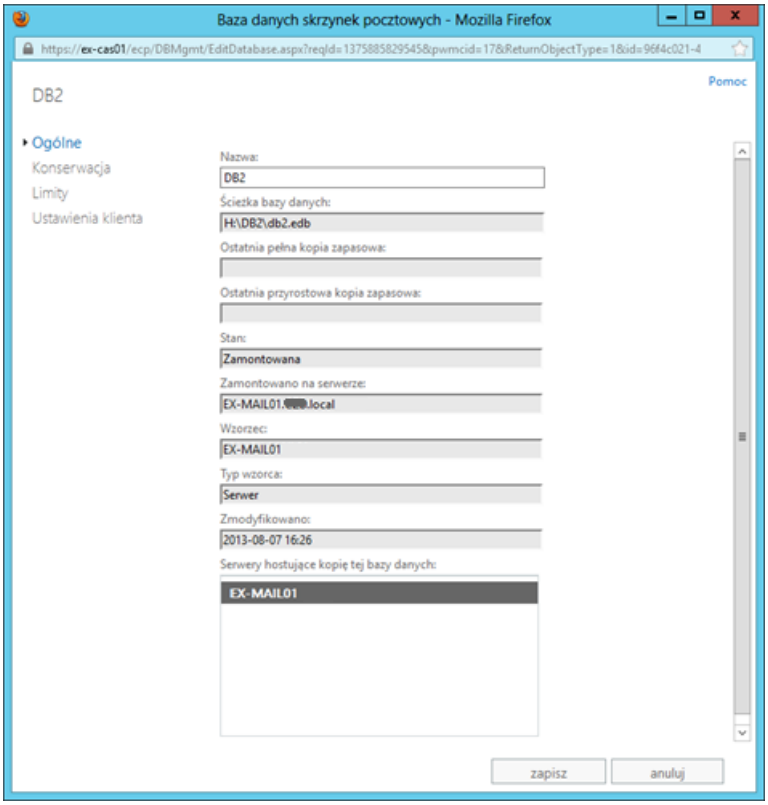


Gdzie:

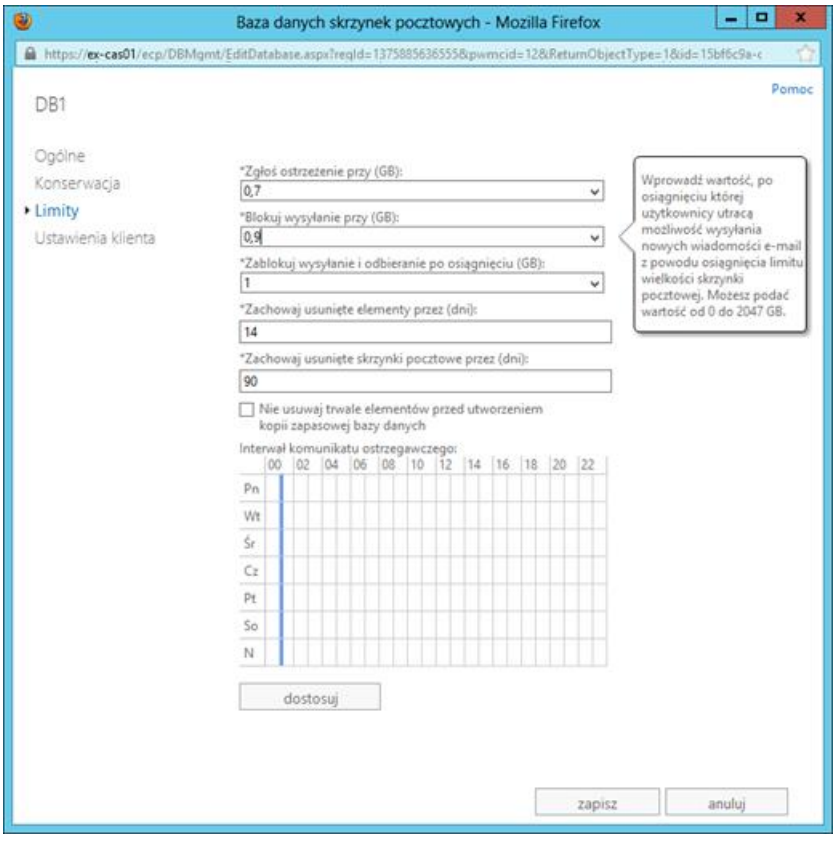
- Baza Danych – Nazwa bazy danych
- Serwer – Serwer, na którym baza zostanie utworzona
- Ścieżka pliku bazy danych – ścieżka pliku bazy danych (musimy wpisać rozszerzenie pliku.EDB)
- Ścieżka folderu dziennika – Ścieżka pliku Log.

Po dodaniu bazy danych należy zrestartować usługę „Microsoft Exchange Infromation Store"

Aby edytować właściwości skrzynki należy zaznaczyć skrzynkę do edycji i wybrać



Następnie przejść do zakładki Limity i postępować zgodnie z rysunkiem:

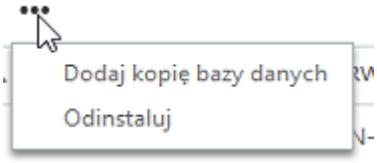


Dodawanie Kopii Bazy Danych

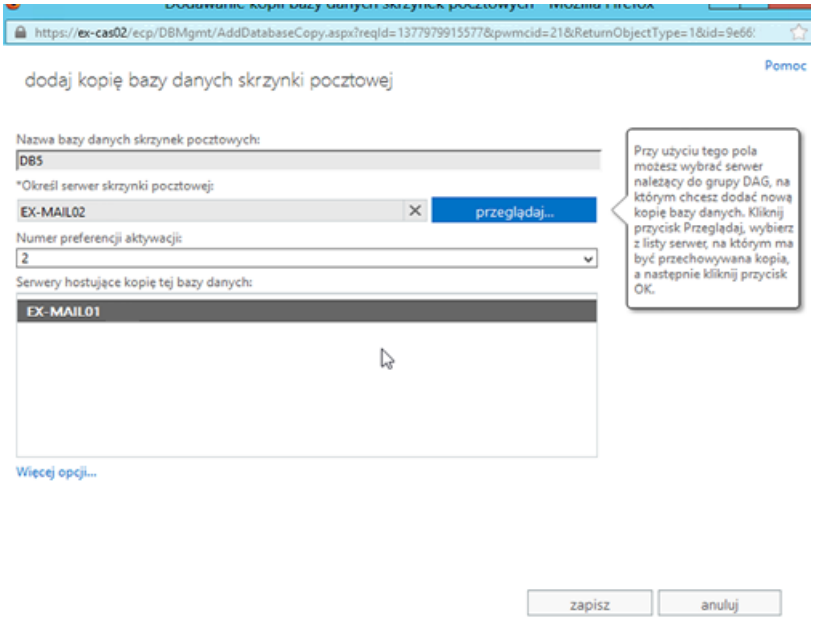
Aby dodać kopię bazy danych do istniejącej już bazy należy zalogować się do Konsoli zarządzania Microsoft Exchange wykorzystując poniższy link:

Https://ex-cas01/ecp

Należy przejść do zakładki „Serwery" → „Bazy danych" i wybrać opcję „Dodaj kopie bazy danych"



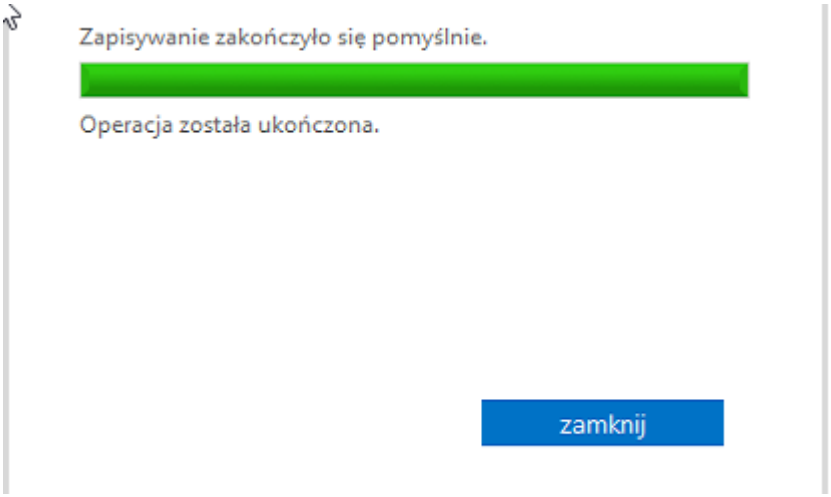
Następnie postępuj zgodnie z rysunkiem



Gdzie:

- Określ serwer skrzynki pocztowej – serwer, na którym ma być kopia bazy danych
- Numer preferencji aktywacji – określa, na którym serwerze baza będzie się pierwsza aktywować po restarcie serwera
- Serwery Hostujące kopię bazy danych – serwer, na którym istnieje już kopia bazy danych

Po wykonaniu kopii pokaże się poniższy komunikat



Po wykonaniu kopii bazy danych można przetestować działanie i funkcjonowanie replikacji używając polecenia PowerShell z Exchange Management Shell wykonując poniższą komendę:

Test-ReplicationHealth

Server	***Check***	***Result***
EX-MAIL01	*ClusterService*	*Passed*
EX-MAIL01	*ReplayService*	*Passed*
EX-MAIL01	*ActiveManager*	*Passed*
EX-MAIL01	*TasksRpcListener*	*Passed*
EX-MAIL01	*TcpListener*	*Passed*
EX-MAIL01	*ServerLocatorService*	*Passed*
EX-MAIL01	*DagMembersUp*	*Passed*
EX-MAIL01	*ClusterNetwork*	*Passed*
EX-MAIL01	*QuorumGroup*	*Passed*
EX-MAIL01	*FileShareQuorum*	*Passed*
EX-MAIL01	*DatabaseRedundancy*	*Passed*
EX-MAIL01	*DatabaseAvailability*	*Passed*
EX-MAIL01	*DBCopySuspended*	*Passed*
EX-MAIL01	*DBCopyFailed*	*Passed*
EX-MAIL01	*DBInitializing*	*Passed*
EX-MAIL01	*DBDisconnected*	*Passed*
EX-MAIL01	*DBLogCopyKeepingUp*	*Passed*
EX-MAIL01	*DBLogReplayKeepingUp*	*Passed*

Certyfikaty

Aby móc wykorzystać w pełni potencjał serwera Exchange i synchronizować pocztę, kalendarz, kontakty z urządzeniami mobilnymi należy zaopatrzyć się w certyfikat SSL wydany przez zaufanego wystawcę (np. Verisign, GeoTrust, Certum itp.). Istotne jest dlatego iż urządzenia mobilne nie połączą się z serwerem chronionym certyfikatem typu selfsign. (Urządzenia oparte na oprogramowaniu Android / Windows Phone).

Kolejną istotną rzeczą jest, aby certyfikat wystawiony typu wildcard posiadał tzw. SAN'y (Subject Alternative Name). SAN to nic innego jak nazwy alternatywne dla serwerów, które będą świadczyły usługi dostępu do poczty Exchange aby mogły być prawidłowe dla świadczenia usług poczty na zewnątrz organizacji (np. ActiveSync, Outlook Anywhere) czy też wewnątrz organizacji (Klienci Outlook).

Innym sposobem na prawidłowy i funkcjonalny certyfikat jest nazwanie domeny, w której funkcjonuje serwer exchange nazwą zewnętrzną domeny (external domain). Wówczas nie jest wymagane podawanie nazw SAN.

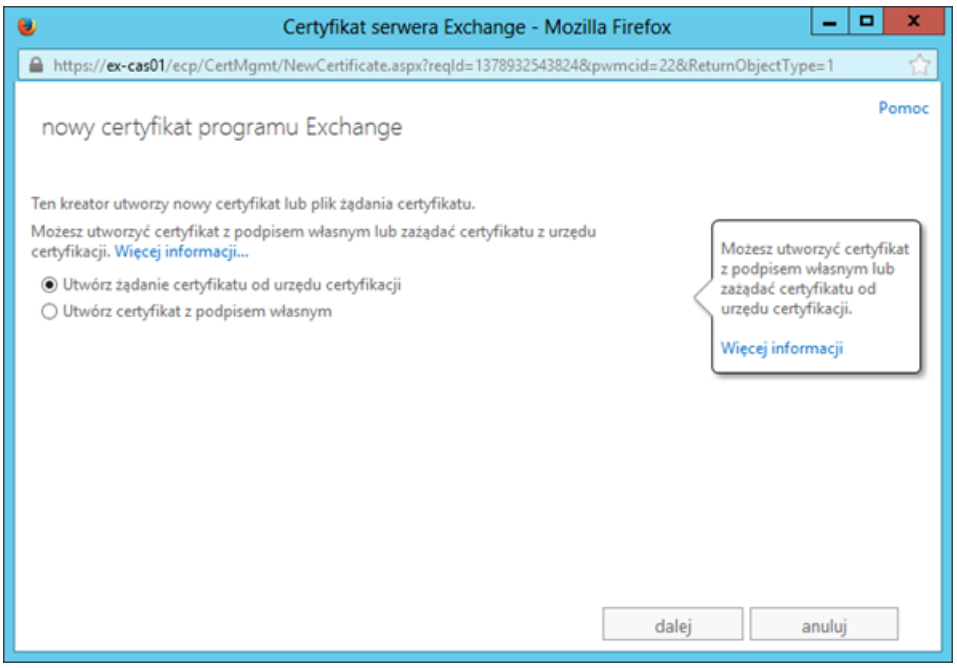
Przygotowanie zamówienia certyfikatu

Przygotowanie zamówienia certyfikatu rozpoczynamy od zalogowania się do konsoli zarządzania serwerem Exchange wykorzystując poniższy link:

Https://ex-cas01/ecp

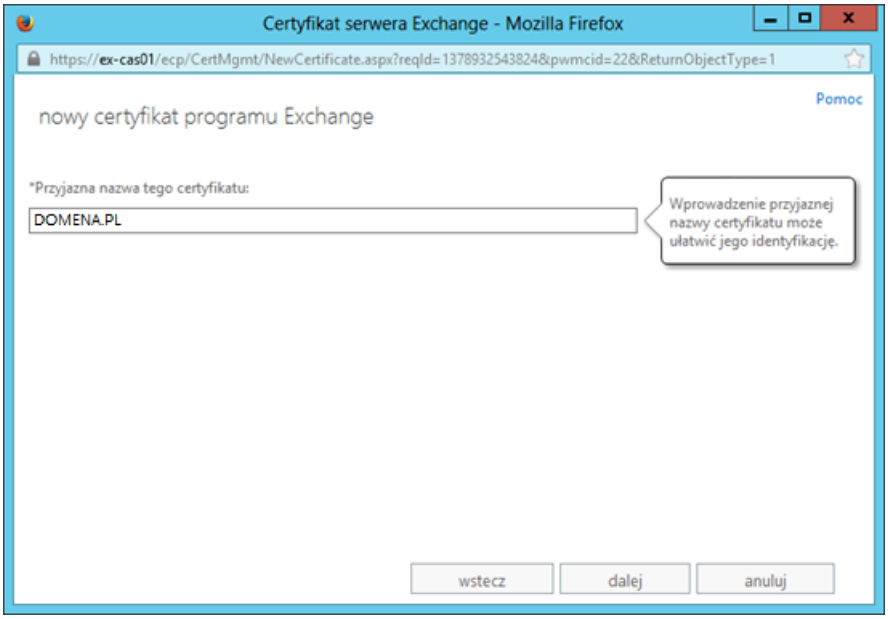
Następnie przechodzimy do opcji *Serwery → Certyfikaty*

Wybieramy + i postępujemy zgodnie z rysunkiem:

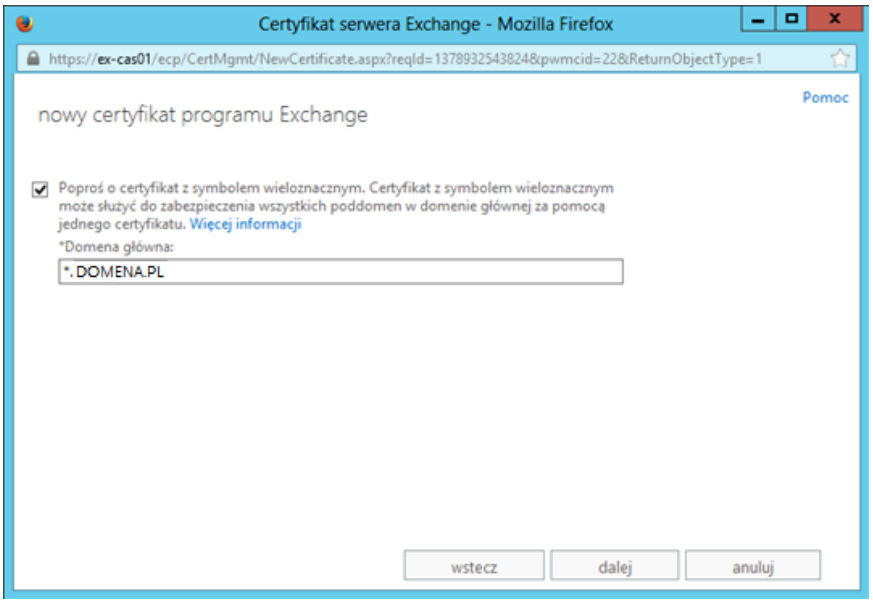


Następnie klikamy *Dalej*.

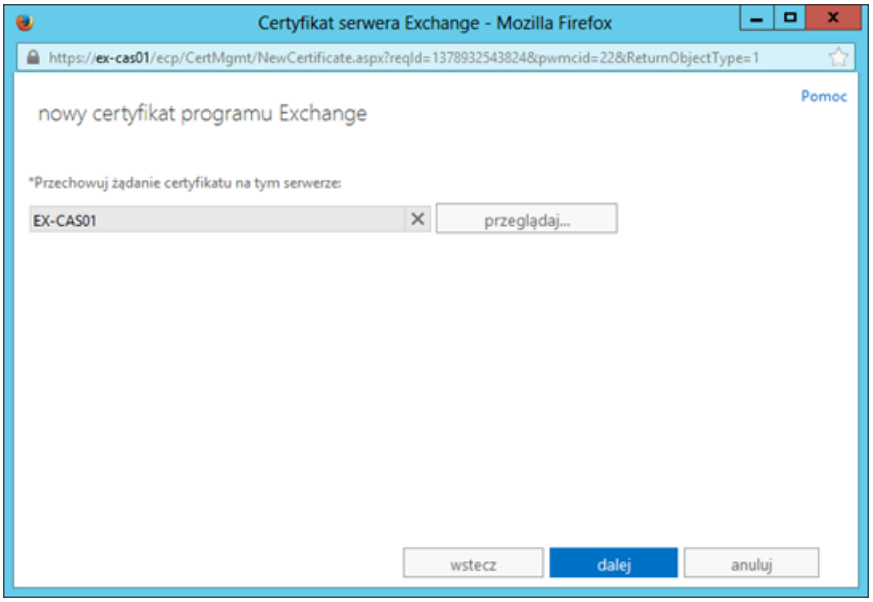
Wybieramy przyjazną nazwę certyfikatu. Nie ma to znaczenia gdyż jest to tylko nazwa identyfikacyjna certyfikatu i klikamy *Dalej.*



Następna strona pozwala nam na zdefiniowanie certyfikatu typu wildcard. Co pozwala zabezpieczyć wiele hostów w jednym drzewie domeny np. *.domena.pl gdzie * to dowolny host w domenie domena.pl. Jest to oszczędność konfiguracyjna jak również finansowa.

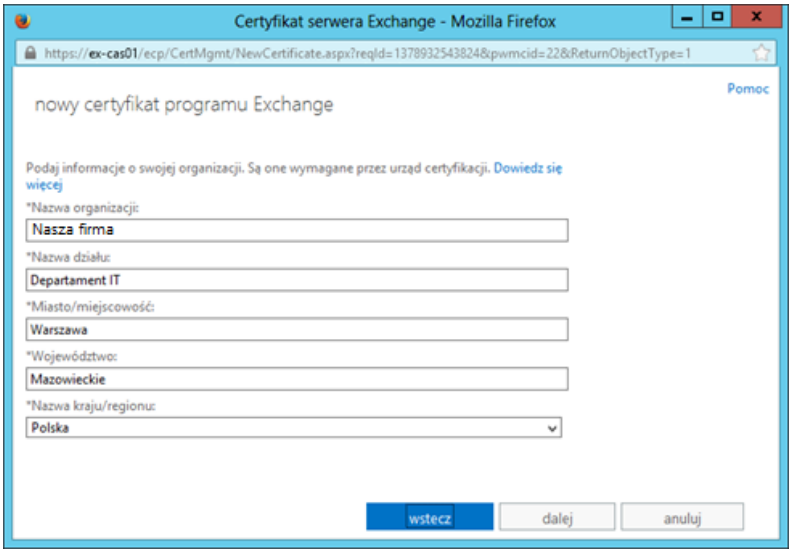


Na kolejnej stronie możemy wybrać serwer, na którym nasze wygenerowane żądanie będzie przechowywane.



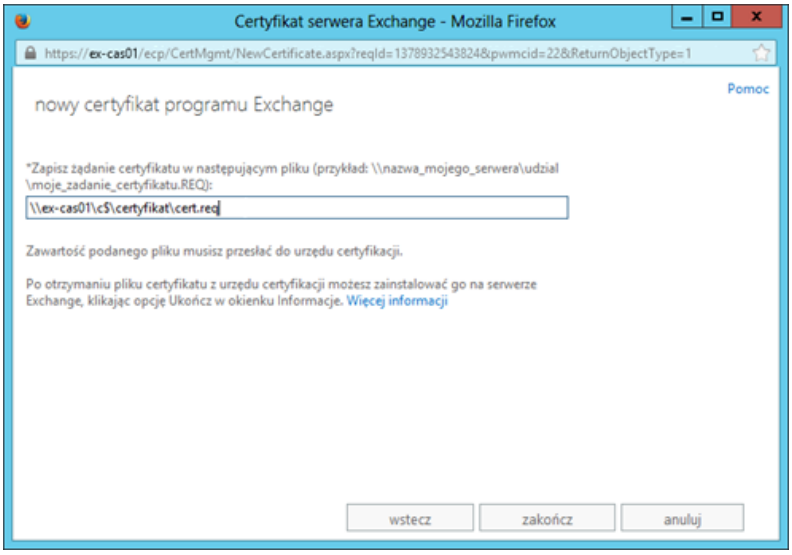
Klikamy *Dalej*

Na kolejnej stronie musimy zdeklarować właściwości wnioskującego o certyfikat



Klikamy *Dalej*

Na ostatniej stronie deklarujemy miejsce zapisania żądania o wydanie certyfikatu.



**Przy generowaniu certyfikatu na stronie portalu np. GeoTrust,Verisign , Certum możemy wybrać wersję certyfikatu z możliwością podania SAN (Subject Alternative Names). Jako SAN'y podajemy nazwy serwerów, na których hostowane są usługi Echange (Client Access Server Role) jak równiez ich nazwy zewnętrzne (np. smtp.domena.pl).* Do SAN'ów dodajemy również host autodiscovery.domena (np. autodiscovery.domena.pl i nazwa domeny wewnętrznej autodiscovery.domena.local).

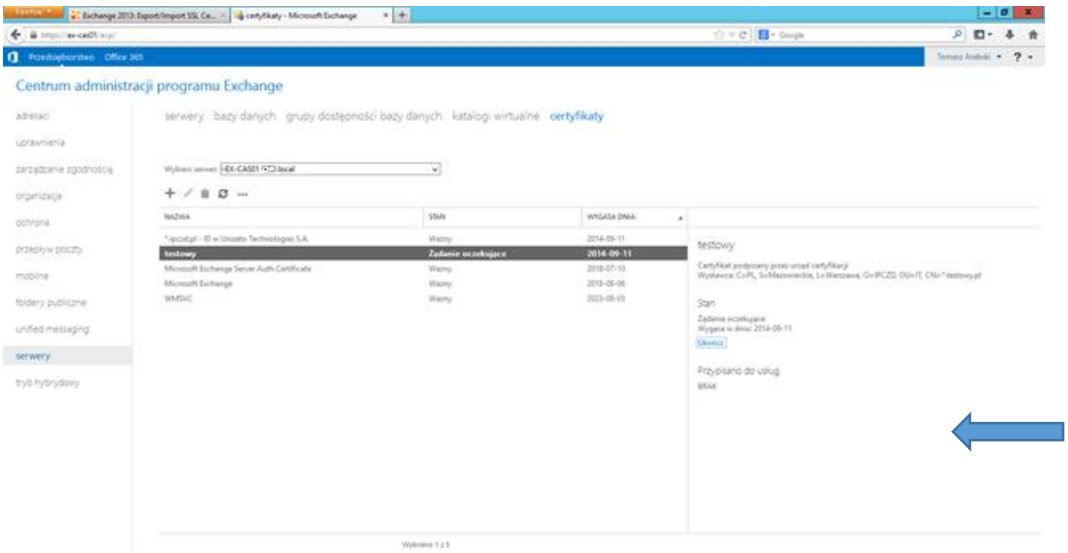
Importowanie przygotowanego certyfikatu

Aby zaimportować wygenerowany certyfikat należy zalogować się do konsoli zarządzanie serwem Exchange

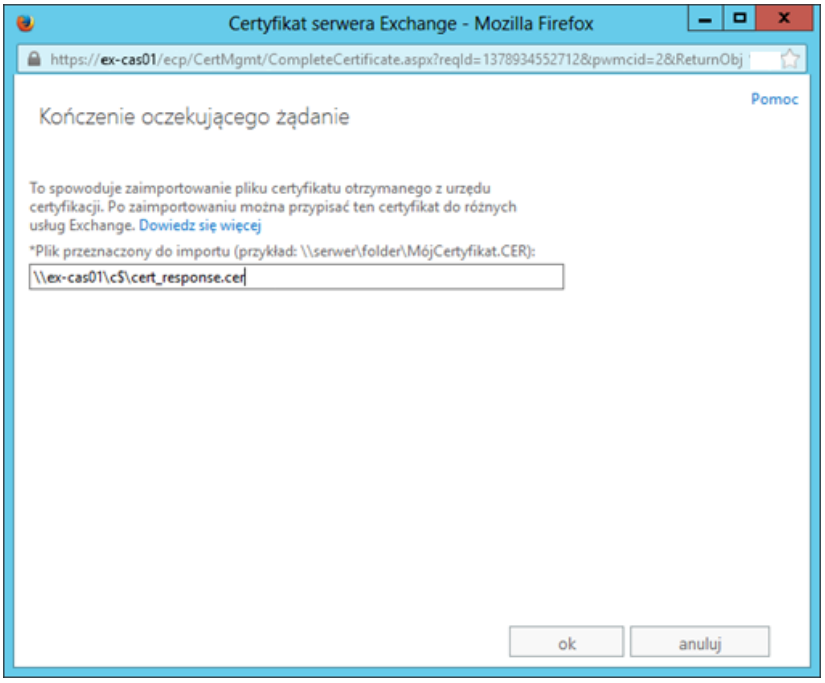
Poprzez poniższy link:
Https://ex-cas01/ecp

Przechodzimy do zakładki *Serwery* → *Certyfikaty* i wybieramy serwer, na którym przygotowywaliśmy wniosek o wydanie certyfikatu.

Wybieramy certyfikat, który przygotowywaliśmy i z prawej części okna klikamy *Ukończ*

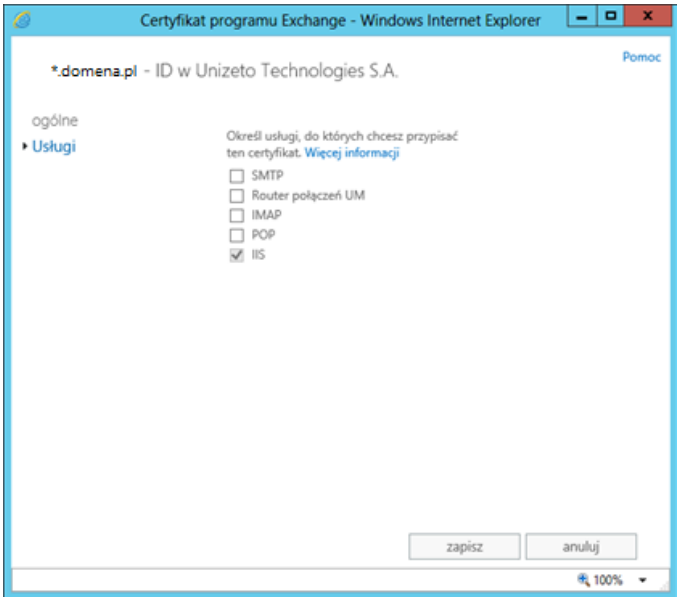


Następnie wpisujemy ścieżkę gdzie zapisaliśmy odpowiedź z centrum certyfikacji



Przypisanie usług do certyfikatu

Aby komunikacja z zewnątrz (z internetu) przebiegała prawidłowo musimy jeszcze przypisać usługi przygotowanemu certyfikatowi należy to wykonać klikając na już zaimportowany certyfikat dwukrotnie i przechodząc do zakładki *Usługi* i następnie klikamy *Zapisz*



Protokoły, porty w systemie

Poprawne działanie usługi poczty elektronicznej jest możliwe wyłącznie po odblokowaniu poniższej komunikacji

Rola EDGE

Usługa	Adres źródłowy	Adres docelowy	Protokół	Port
SMTP	Wszystkie serwery Edge Transport	Wszystkie serwery Hub Transport:	TCP	25 SMTP
SMTP	Wszystkie serwery Edge Transport	Wszystkie serwery Edge Transport	TCP	25 SMTP
SMTP	Wszystkie serwery Edge Transport	Wszystkie adresy w Internecie	TCP	25 SMTP – opcjonalnie, na wypadek przełączenia Edge w tryb wysyłania bezpośrednio do Internetu
Aktualizacja systemu ForeFront Protection	Wszystkie serwery Edge Transport	Wszystkie adresy w Internecie	TCP	80 http

Tabela: Komunikacja serwerów transport brzegowego (Edge)

Rola Hub

Usługa	Adres źródłowy	Adres docelowy	Protokół	Port
SMTP	Wszystkie serwery Hub Transport	Wszystkie serwery Hub Transport	TCP	25 SMTP
SMTP	Wszystkie serwery Hub Transport	Wszystkie serwery Edge Transport	TCP	25 SMTP
MS Exchange Mail Submission	Wszystkie serwery Mailbox	Wszystkie serwery Hub Transport	TCP	135 RPC
MS Exchange Mail Submission	Wszystkie serwery Mailbox	Wszystkie serwery Hub Transport	TCP	1024-65535 RPC dynamic
MAPI	Wszystkie serwery Hub Transport	Wszystkie serwery Mailbox	TCP	135 RPC
MAPI	Wszystkie serwery Hub Transport	Wszystkie serwery Mailbox	TCP	1024-65535 RPC dynamic

Exchange EdgeSync	Wszystkie serwery Hub Transport	Wszystkie serwery Edge Transport	TCP	Secure LDAP 50636
Active Directory Access	Wszystkie serwery Hub Transport	Wszystkie kontrolery domeny w lokacji xxxx	TCP/UDP	389 LDAP 88 Kerberos 53 DNS
Active Directory Access	Wszystkie serwery Hub Transport	Wszystkie kontrolery domeny w lokacji xxxx	TCP	3268 LDAP GC 135 RPC
SMTP	Wewnętrzny klient SMTP (wewnętrzne aplikacje, serwery wysyłające pocztę na serwery Exchange)	Wszystkie serwery Hub Transport	TCP	587 SMTP 25 SMTP
Pobieranie aktualizacji ForeFront	Wszystkie serwery Hub Transport	Wszystkie serwery Edge Transport	TCP	80 http

Tabela: Komunikacja serwerów transportu

Rola Mailbox

Usługa	Adres źródłowy	Adres docelowy	Protokół	Port
Active Directory Access	Wszystkie serwery Mailbox	Kontrolery domeny w lokacji xxxx	TCP/UDP	389 LDAP 88 Kerberos 53 DNS
Active Directory Access	Wszystkie serwery Mailbox	Kontrolery domeny w lokacji xxxx	TCP	3268 LDAP GC 135 RPC 1024-65535 RPC dynamic
Remote Registry	Stacja zarządzająca (sdministracyjna)	Wszystkie serwery Mailbox	TCP	135 RPC 1024-65535 RPC dynamic

SMB	Stacja zarządzająca (sdministracyjna)	Wszystkie serwery Mailbox	TCP	445 SMB
Availablity Web Service	Wszystkie serwery Client Acces	Wszystkie serwery Mailbox	TCP	135 RPC 1024-65535 RPC dynamic
Clustering	Wszystkie serwery Mailbox	Wszystkie serwery Mailbox	TCP	135 RPC 1024-65535 RPC dynamic
Clustering	Wszystkie serwery Mailbox	Wszystkie serwery Mailbox	UDP	3343
Content Indexing	Wszystkie serwery Client Access	Wszystkie serwery Mailbox	TCP	135 RPC 1024-65535 RPC dynamic
Log Shipping	Wszystkie serwery Mailbox	Wszystkie serwery Mailbox	TCP	64327
Seeding	Wszystkie serwery Mailbox	Wszystkie serwery Mailbox	TCP	64327
VSS backup	Serwer kopii zapasowych	Wszystkie serwery Mailbox	TCP	445 SMB
Mailbox Assistants	Wszystkie serwery Client Access	Wszystkie serwery Mailbox	TCP	135 RPC 1024-65535 RPC dynamic
MAPI	Wszystkie serwery Client Access	Wszystkie serwery Mailbox	TCP	135 RPC 1024-65535 RPC dynamic
Active Directory Topology	Wszystkie serwery Mailbox	Kontrolery domeny w lokacji xxxx	TCP	135 RPC 1024-65535 RPC dynamic
Exchange System Attendant	Wszystkie serwery Mailbox	Wszystkie serwery Mailbox	TCP	135 RPC

				1024-65535 RPC dynamic
Exchange System Attendant	Wszystkie serwery Serwer Mailbox	Kontrolery domeny w lokacji xxxx	TCP/UDP	389 LDAP 88 Kerberos 53 DNS
Exchange System Attendant	Wszystkie serwery Mailbox	Kontrolery domeny w lokacji xxxx	TCP	3268 LDAP GC 135 RPC 1024-65535 RPC dynamic
Offline Address Book	Wszystkie serwery Mailbox	Kontrolery domeny w lokacji xxxx	TCP	135 RPC 1024-65535 RPC dynamic
Dostęp do OAB	Wszystkie serwery Client Access	Wszystkie serwery Mailbox	TCP	80 http 443 HTTPS
Dostęp do Recipient Update service	Wszystkie serwery Client Access	Wszystkie serwery Mailbox	TCP	135 RPC 1024-65535 RPC dynamic

Tabela: Komunikacja serwerów Mailbox

Rola CAS

Usługa	Adres źródłowy	Adres docelowy	Protokół	Port
Active Directory Access	Wszystkie serwery Client Access	Kontrolery domeny w lokacji xxxx	TCP/UDP	389 LDAP 88 Kerberos 53 DNS
Active Directory Access	Wszystkie serwery Client Access	Kontrolery domeny w lokacji xxxx	TCP	3268 LDAP GC 135 RPC 1024-65535 RPC dynamic

MAPI	Klient poczty	Wszystkie serwery Client Access	TCP	135 RPC 6005-59530 RPC dynamic
Autodiscover	Klient poczty	Wszystkie serwery Client Access	TCP	80 http 443 HTPS
Availability	Klient poczty	Wszystkie serwery Client Access	TCP	80 http 443 HTPS
Outlook Web App	Klient poczty	Wszystkie serwery Client Access	TCP	80 http 443 HTPS
POP3	Klient poczty	Wszystkie serwery Client Access	TCP	110 TLS 995 SSL
IMAP4	Klient poczty	Wszystkie serwery Client Access	TCP	143 TLS 993 SSL
Outlook Anywhere	Klient poczty	Wszystkie serwery Client Access	TCP	80 http 443 HTPS
Exchange Activesync	Klient poczty	Wszystkie serwery Client Access	TCP	80 http 443 HTPS
MAPI	Wszystkie serwery Client Access	Wszystkie serwery Mailbox	TCP	135 RPC 1024-65535 RPC dynamic
Exchange Activesync	Wszystkie serwery Client Access	Wszystkie serwery Client Access	TCP	80 http 443 HTPS
Outlook Web Access	Wszystkie serwery Client Access	Wszystkie serwery Client Access	TCP	80 http 443 HTPS
Exchange Web Services	Wszystkie serwery Client Access	Wszystkie serwery Client Access	TCP	443 HTPS

POP3, (jeżeli miałby być uruchomiony)	Wszystkie serwery Client Access	Wszystkie serwery Client Access	TCP	995 SSL
IMAP4, (jeżeli miałby być uruchomiony)	Wszystkie serwery Client Access	Wszystkie serwery Client Access	TCP	993 SSL

Tabela: Komunikacja serwerów CAS

Uwaga: Domyślnie usługa MAPI korzysta z RPC i na serwerze Client Access Server (zainstalowanym na serwerze Windows 2008 lub Windows 2008 R2) wykorzystuje port TCP 135 oraz dynamiczny zakres portów TCP 6005-59530

Dla ułatwienia konfiguracji urządzeń równoważących obciążenie możliwe jest ograniczenie dynamicznego zakresu portów wykorzystywanych przez RPC na serwerze w roli Client Access Server na każdym serwerze do dwóch portów statycznych.

W przypadku skonfigurowania statycznym portów dla usługi RPC konieczne jest otwarcie tych portów na urządzeniach firewall pomiędzy klientami i serwerami a także skonfigurowanie równoważenia obciążenia tych portów w klastrze NLB. Po skonfigurowaniu statycznych portów zakres dynamiczny dla połączeń klientów do serwerów w rolach CAS nie jest wykorzystywany i może być wyłączony w klastrze NLB oraz na urządzeniach firewall.

Lync

Microsoft Lync to ujednolicona platforma komunikacyjna przystosowana do wykorzystania w przedsiębiorstwach. Lync pozwala kontaktować się ze sobą ludziom z różnych części świata za pomocą urządzeń mobilnych z systemem Windows 8 i innymi systemami operacyjnymi podczas wykonywania codziennych obowiązków. Dzięki niemu użytkownicy korzystają z tego samego narzędzia do informowania o obecności w pracy, przesyłania komunikatów, połączeń głosowych i wideo oraz spotkań online. Mogą też skontaktować się z milionami użytkowników programu Skype na całym świecie.

Istnieje kilka najważniejszych funkcji w Lync Server, które wpływają na bezpieczeństwo produktu

Uwierzytelnianie numerem PIN

Działanie funkcji. Uwierzytelnianie numerem PIN to mechanizm używany do uwierzytelniania użytkowników dołączających do spotkań automatycznej recepcjonistki konferencji oraz uwierzytelniania użytkowników wdrażających po raz pierwszy program Microsoft Lync Phone Edition. Użytkownik wprowadza numer telefonu lub numer wewnętrzny oraz numer PIN używany przez program Lync Server do sprawdzania poprawności poświadczeń użytkownika. Numer PIN może zostać ustawiony przez użytkownika lub podany przez administratora przedsiębiorstwa.

Informacje zbierane, przetwarzane lub przesyłane. Podczas uwierzytelniania zbierany jest numer telefonu lub numer wewnętrzny i numer PIN użytkownika. Program Lync Server sprawdza poprawność tych informacji w swojej bazie danych. Ze względów bezpieczeństwa numer PIN jest zapisywany w wewnętrznej bazie danych w postaci nieodwracalnego skrótu. Po ustawieniu numer PIN nie jest widoczny dla żadnej osoby. Numer PIN może zostać ustawiony lub zresetowany przez użytkownika, administratora lub pracownika pomocy technicznej.

Gdy administrator lub pracownik pomocy technicznej ustawia lub resetuje numer PIN, nowy numer PIN jest wyświetlany i opcjonalnie może zostać przesłany użytkownikowi w wiadomości e-mail. Dostępny szablon wiadomości e-mail, który można dostosować, zawiera tekst informujący użytkownika, że numer PIN mógł zostać wyświetlony przez administratora lub pracownika pomocy technicznej, więc zaleca się jego zmianę.

Wybór i kontrola: Ta funkcja jest domyślnie włączona. Administrator przedsiębiorstwa może wyłączyć uwierzytelnianie numerem PIN na stronie ustawień zabezpieczeń panelu sterowania programu Lync Server, zaznaczając opcję Uwierzytelnianie numerem PIN.

Włączenie funkcji PIN możliwe jest między innymi za pomocą PowerShell

Set-CsWebServiceConfiguration -Identity Global -UsePinAuth $true

Przypisanie losowego numeru PIN dla wybranego użytkownika wykonać można za pomocą polecenia PowerShell:

Set-CsClientPin -Identity "litwareinc\kenmyer"

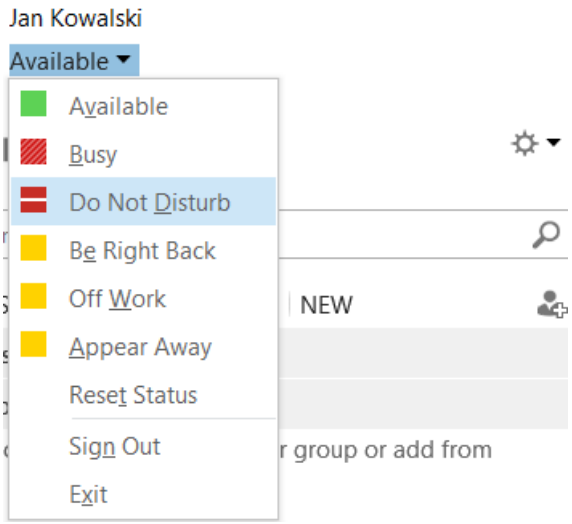
Określenie konkretnego numeru PIN dla wybranego użytkownika za pomocą polecenia:

Set-CsClientPin -Identity "litwareinc\kenmyer" -Pin 18723834

Tryb prywatności

Tryb prywatności to ustawienie, które pozwala użytkownikowi określić, ile informacji o swojej obecności (takich jak Dostępny, Zajęty czy Nie przeszkadzać) chce udostępniać osobom ze swojej listy kontaktów.

Informacje zbierane, przetwarzane lub przesyłane: Włączenie trybu prywatności powoduje przejście programu Lync w tryb, w którym użytkownik może tak dopasować swoje ustawienia, aby informacje o jego obecności były udostępniane tylko kontaktom z listy kontaktów.



Administrator przedsiębiorstwa może zdecydować się na włączenie trybu prywatności na poziomie puli (korzystając z ustawienia wewnątrzpasmowego EnablePrivacyMode). Po jego włączeniu domyślnie wszyscy użytkownicy końcowi programu Lync będą przełączani w tryb prywatności przy logowaniu.

W przypadku włączenia trybu prywatności na serwerze przez ustawienie administratora użytkownicy końcowi mogą zdecydować się na wyświetlanie swojej obecności wszystkim osobom (tryb standardowy) lub tylko swoim kontaktom (tryb prywatności).

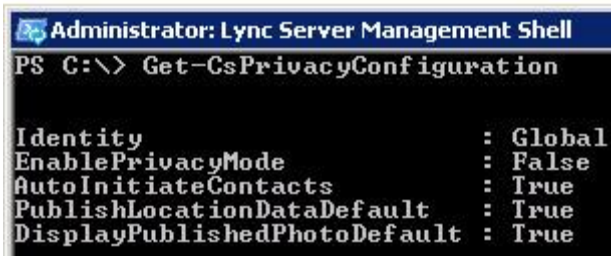
W przypadku włączenia na serwerze trybu standardowego przez ustawienia administratora użytkownicy końcowi nie mogą przełączać się w tryb prywatności. Mogą pracować jedynie w trybie standardowym. Mogą jednak wstępnie zrezygnować z trybu prywatności, dzięki czemu w przypadku ustawienia trybu prywatności przez administratora nie zostaną przełączeni w tryb prywatności przy następnym logowaniu do programu Lync.

Włączenie zaawansowanego trybu prywatności możliwe jest za pomocą polecenia:

Get-CsPrivacyConfiguration | Set-CsPrivacyConfiguration -EnablePrivacyMode $True

Sprawdzenie statusu konfiguracji możliwe jest za pomocą polecenia:

Get-CsPrivacyConfiguration



Kontrola dostępu oparta na rolach

Funkcja kontroli dostępu opartej na rolach (RBAC, Role Based Access Control) umożliwia delegowanie uprawnień administracyjnych na potrzeby scenariuszy administratorów przedsiębiorstwa. Interakcja administratora przedsiębiorstwa z interfejsami zarządzania może być ograniczona do konkretnie dozwolonych operacji i obiektów dostępnych do modyfikowania.

Informacje zbierane, przetwarzane lub przesyłane: Możliwości dostępne administratorowi przedsiębiorstwa są oceniane w czasie wykonywania na podstawie członkostwa w grupach użytkowników, a konkretnie w grupach zabezpieczeń usługi Active Directory. Możliwości roli w systemie są konfigurowane i ustawiane na centralnym serwerze zarządzania.

Wykorzystywanie informacji: Administrator przedsiębiorstwa może skonfigurować dodatkowe role administratorów RBAC dla danego wdrożenia. Administrator przedsiębiorstwa może wyświetlać wszystkie role, do których należą inni administratorzy.

Wybór i kontrola: To jest mechanizm zabezpieczeń/autoryzacji do zadań zarządzania infrastrukturą informatyczną. Ta funkcja nie wpływa na użytkowników końcowych ani na widoczne dla nich informacje.

Aby skorzystać z RBAC należy użyć polecenia:

Set-CsAdminRole

Przykład dodania użytkowników do roli RedmondVoiceAdministrators z OU Portland.

Set-CsAdminRole -Identity "RedmondVoiceAdministrators" -UserScopes @{Add="OU:ou=Portland,dc=litwareinc,dc=com"}

Te same czynności możliwe są do wykonania z poziomu konsoli administracyjnej Active Directory Users and Computers.

W systemie zdefiniowanych jest kilka standardowych ról:

- CsAdministrator
- CsUserAdministrator
- CsVoiceAdministrator
- CsServerAdministrator
- CsViewOnlyAdministrator
- CsHelpDesk
- CsArchivingAdministrator

- CsResponseGroupAdministrator
- CsLocationAdministrator

Server-to-Server Authentication

W Lync 2013 proces autentykacji może być skonfigurowany pomiędzy serwerami za pomocą protokołu Open Authorization (OAuth). Za pomocą tego protokoły dwa serwery, np. Lync i Exchange, mogą mieć skonfigurowaną relację zaufania. Dzięki temu integracja różnych produktów staje się dużo łatwiejsza. Lync Server 2013 musi mieć możliwość bezpiecznej i przejrzystej komunikacji z innymi aplikacjami oraz serwerami.

Możliwa jest komunikacji typu Lync-SharePoint oraz Lync-Exchange, ale również ze stronami Web oraz innymi aplikacji, które wspierają lub używają protokołu OAuth a co za tym idzie nawiązać relację zaufania między nimi a serwerem Lync 2013.

Aby sprawdzić czy na serwerze Lync ustawiona jest autentykacja OAuth należy wykonać polecenie:

Get-CsCertificate -Type OAuthTokenIssuer

Jeśli nie zostanie zwrócona żadna informacja – czyli nie był przypisany żaden certyfikat należy go przypisać. Są dwie podstawowe zasady, które są istotne z punktu widzenia autentykacji server-to-server:

- ten sam certyfikat musi być skonfigurowany jako certyfikat OAuthTokenIssuer na wszystkich serwerach FrontEnd
- certyfikat musi być co najmniej 2048 bitowy

Instalacja certyfikatu wymaga polecenia:

Import-CsCertificate -Identity global -Type OAuthTokenIssuer -Path C:\Certificates\ServerToServerAuth.pfx -Password "P@ssw0rd"

Po instalacji certyfikatu należy skonfigurować tzw. aplikację partnerską – np. Exchange Server lub SharePoint. Do tego celu należy użyć poniższego skryptu:

```
if ((Get-CsPartnerApplication -ErrorAction SilentlyContinue) -ne $Null)
  {
    Remove-CsPartnerApplication app
  }

$exch = Get-CsPartnerApplication microsoft.exchange -ErrorAction SilentlyContinue
if ($exch -eq $null)
  {
    New-CsPartnerApplication -Identity microsoft.exchange -MetadataUrl https://atl-exchange-001.litwareinc.com/autodiscover/metadata/json/1 -ApplicationTrustLevel Full
```

```
  }
else
  {
    if ($exch.ApplicationIdentifier -ne "00000002-0000-0ff1-ce00-000000000000")
      {
        Remove-CsPartnerApplication microsoft.exchange
New-CsPartnerApplication -Identity microsoft.exchange -MetadataUrl https://atl-exchange-
001.litwareinc.com/autodiscover/metadata/json/1 -ApplicationTrustLevel Full
      }
     else
      {
        Set-CsPartnerApplication -Identity microsoft.exchange -ApplicationTrustLevel Full
      }
  }

$shp = Get-CsPartnerApplication microsoft.sharepoint -ErrorAction SilentlyContinue
if ($shp -eq $null)
 {
   New-CsPartnerApplication -Identity microsoft.sharepoint -MetadataUrl http://atl-sharepoint-
001.litwareinc.com/jsonmetadata.ashx -ApplicationTrustLevel Full
  }
else
  {
    if ($shp.ApplicationIdentifier -ne "00000003-0000-0ff1-ce00-000000000000")
      {
        Remove-CsPartnerApplication microsoft.sharepoint

        New-CsPartnerApplication -Identity microsoft.sharepoint -MetadataUrl http://atl-sharepoint-
001.litwareinc.com/jsonmetadata.ashx -ApplicationTrustLevel Full
      }
     else
      {
        Set-CsPartnerApplication -Identity microsoft.sharepoint -ApplicationTrustLevel Full
       }
 }
Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-000000000000
```

Lync Server 2013 Best Practices Analyzer

W celu zapewnienia bezpiecznej instalacji i konfiguracji warto rozważyć użycie narzędzi wspierających prace administratora systemu. Jednym z takich narzędzi jest Best Practices Analyzer, który potrafi przeanalizować konfigurację i instalację o znaleźć potencjalne problemy.

Best Practices Analyzer jest w stanie przetestować serwery, na których uruchiomione są następujące usługi:

- Active Directory Domain Services
- Exchange Server Unified Messaging (UM)
- Lync Server.

Best Practices Analyzer może być użyty do:

- Proaktywnego sprawdzenia konfiguracji i jej zgodności z rekomendowanymi najlepszymi praktykami
- Automatycznie wykrywać wymagane aktualizacje dla Lync Server 2013
- Wygenerować listę problemów jak nieoptymalna konfiguracja ustawień, niewspierane opcje, brak aktualizacji oraz sprawdzić co nie jest rekomendowane
- Wykryć i naprawić specyficzne problemy

Przykładowy ekran po zakończeniu skanowania